КОМПЬЮТЕР ТИЗИМЛАРИДА АХБОРОТЛАРНИ ҲИМОЯЛАШ ФАНИДАН МАЖМУА

Ҳ.Урдушев, М.Рахимов

Компьютер тизимларида ахборотларни ҳимоялаш фанидан амалий, лаборатория иши ва мустақил таълим вазифаларини бажариш учун

М А Ж М У А

«Иқтисодиёт» ва «Фермер хўжалигини бошқариш» йўналишларида таълим олаётган бакалавлар учун

Самарқанд 2009

ЎЗБЕКИСТОН РЕСПУБЛИКАСИ ҚИШЛОҚ ВА СУВ ХЎЖАЛИГИ ВАЗИРЛИГИ
САМАРҚАНД ҚИШЛОҚ ХЎЖАЛИГИ ИНСТИТУТИ
ОЛИЙ МАТЕМАТИКА ВА АХБОРОТ ТЕХНОЛОГИЯЛАРИ КАФЕДРАСИ

КОМПЬЮТЕР ТИЗИМЛАРИДА АХБОРОТЛАРНИ ҲИМОЯЛАШ ФАНИДАН АМАЛИЙ, ЛАБОРАТОРИЯ ИШИ ВА МУСТАҚИЛ ТАЪЛИМ ВАЗИФАЛАРИНИ БАЖАРИШ УЧУН МАЖМУА.

«Иқтисодиёт» ва «Фермер хўжалигини бошқариш» йўналишларида таълим олаётган бакалаврлар учун

Тузувчилар: доцент Ҳ.Урдушев, доцент М.Н.Рахимов
Тақризчилар: доцент З.Махмудов (ТАТУ Самарқанд филали),
катта ўқитувчи Абдулаҳад Рахимов (СамҚХИ).

Мажмуа «Олий математика ва ахборот технологиялари кафедраси компьютерларида терилиб сахифаланган ва кўпайтирилган. Самарқанд 2009 йил. 108 бет.

М у н д а р и ж а

I.Компьютер тизимларида ахборотларни ҳимоялаш фан дастури 5

II.Компьютер тизимларида ахборотларни ҳимоялаш фанидан ишчи ўқув дастури 10
II.1.Маъруза машғулотларининг мавзулари 11
II.2.Амалий машғулот ва лаборатория ишлари мавзулари 12
II.3.Мустақил таълим мавзулари 13
II.4 «Компьютер тизимида ахборотларни ҳимоялаш» фанидан якуний баҳолаш саволари 14
II.5.Фан бўйича адабиётлар рўйхати ва интернет ахборот ресурсларидаги электрон версияларининг номи 16
II.6.Фан бўйича талабаларни баҳолаш тартиби 17

1. Мавзу. Windows операцион тизимини паролли ҳимоялаш 18
1.1.Операцион тизимларни паролли ҳимоялаш 18
1.2. Паролларни ўрнатиш ва олиб ташлаш 20
2.Мавзу. Windows операцион тизимида файл ва папкалар тузиш, нусхаларини яратиш ва архивлаш 22
2.1.Windows XP папка ва файллар яратиш 22
2.2. Папка ва файллар нусхаларини яратиш 23
2.3. Архиватор дастурлари 24
2.4. Windows XP папка ва файлларни архивлаш 24
2.5. Архивланган папка ва файлни очиш 27
3.Мавзу. Windows XP иловалари паролли ҳимоялаш 29
3.1. Microsoft Word дастурида файллар тузиш ва уларга парол ўрнатиш 29
3.2. Microsoft Excel дастурида файллар тузиш ва уларга парол ўрнатиш 30
3.3. Компьютерда вазифалар бажариш 32
4. Мавзу. Антивирус дастурлари 33
4.1.Антивирус дастурлари ҳақида 33
4.2. NOD32 антивирус дастури 34
4.3. Касперского Personal антивирус дастури 36
4.4. Антивирус дастурлари билан ишлаш 37
5.Мавзу. Ахборотларни стенографик ҳимоялаш усуллари Ахборотларни шифрлашда ўринларни алмаштириш усули 40
5.1. Ахборотларни ўринларни алмаштириш усули билан шифрлаш 40
5.2. Ахборотларни таянч сўзли ўринларни алмаштириш усули билан шифрлаш 42
Амалий машғулот вазифалари 45
Лаборатория иши вазифалари 47
6. Мавзу. Ахборотларни стенографик ҳимоялаш усуллари. Ахборотларни шифрлашни Цезар усули 49
6.1. Ахборотларни Цезар усули билан шифрлаш 49
6.2. Ахборотларни аффин тизимидаги Цезар усули билан шифрлаш 50
6.3. Таянч сўзли Цезар усули 53

Лаборатория иши вазифалари 54
Мустақил таълим вазифалари 55
7.Мавзу. Ахборотларни гаммалаш усули билан шифрлаш 56
7.1. Таққосламалар ҳақида асосий тушунчалар 56
7.2. Ахборотларни гаммалаш усули билан шифрлаш 57
Амалий машғулот вазифалари 60
Лаборатория иши вазифалари 62
8.Мавзу. Ахборотларни симметрик усул билан шифрлаш. Вижинер усули 63
8.1.Ахборотларни Вижинер жадвали билан оддий шифрлаш 64
8.2. Ахборотларни Вижинер жадвали билан калитли шифрлаш 65
Амалий машғулот вазифалари 68
Лаборатория иши вазифалари 72
Мустақил таълим вазифалари 74
9.Мавзу. Ахборотларни криптографик ҳимоялашни аналитик усуллари. Хилл усули 75
9.1.Хилл усули билан ахборотларни шифрлаш 75
9.2.Хилл усули билан ахборотларни дешифрлаш 76
Амалий машғулот вазифалари 80
Лаборатория иши вазифалари 84
Мустақил таълим вазифалари 88

Мустақил таълим учун материаллар 93

Мавзу. Вирусларнинг файллар таркибига таъсири 93
Файллар таркибини бузувчи ва бузмайдиган вируслар 93
Оператор курилмаларига таъсир этувчи вируслар 94
Мавзу. Ташкилотларда ахборотларни ҳимоялаш 96
Ташкилотлардаги ахборотларни ҳимоялаш 96
Ахборотларни ташкилий ҳимоялаш элементлари 96
Ахборот тизимларида маълумотларга нисбатан хавф-хатарлар 97
Мавзу. Электрон тўловлар тизимида ахборотларни ҳимоялаш 99
Электрон тўловлар тизими асослари 99
Идентификацияловчи шахсий номерни ҳимоялаш 100
Банкоматлар хавфсизлигини таъминлаш 101
Internetда мавжуд электрон тўловлар хавфсизлигини таъминлаш 102
Мавзу. Компьютер тизимларининг ҳимояланганлик даражасини аниқлаш воситалари 103
Компьютер тизимларининг ҳимояланганлик даражасини аниқлаш воситалари 103
SSS(System Secyrity Scanner) дастури 103
Internet Scanner SAFFEsuite дастури ҳақида 104

I.Компьютер тизимларида ахборотларни ҳимоялаш ФАН ДАСТУРИ

Олий таълимнинг:600000 Қишлоқ хўжалиги билим соҳасининг 5340100 - "Иқтисодиёт (қишлоқ хўжалиги)" 5541000 - "Фермер хўжаликларини бошқариш" бакалавр йўналишлари учун.
Самарқанд -2006

Тузувчилар: иқтисод фанлари номзоди, доцент Ҳ.Урдушев,
иқтисод фанлари номзоди, доцент М.Н.Рахимов

Такризчилар: иқтисод фанлари номзоди, доцент – Б.И.Усманов (СамДУ), техника фанлари номзоди, доцент – И.Абруев (СамҚХИ)

Фан дастури: Самарқанд қишлоқ хўжалик институти ректори томонидан (30. 08. 2006 й.) тасдиқланган (Проф. Ш.Т.Ҳолиқулов)

Самарқанд қишлоқ хўжалик институти марказий аттестация ва услубий кенгашининг 30. 08. 2006 йилдаги №1 сонли мажлис баённомаси билан тасдиқланган(Кенаш раиси, профессор Т.Э.Остонақулов)

"Иқтисодиёт ва бошқарув" факултети услубий кенгаши йиғилишида муҳокама қилинган ва 29.08.2006 йилдаги №1- сонли баённомаси билан тасдиққа тавсия этилган (Факультет илмий – услубий кенгаши раиси, доцент Т.Қ.Қудратов).

"Олий математика ва ахборот технологиялари" кафедраси йиғилишида муҳокама қилинган ва 2006 йил 19.05.2006 йилдаги 10- сонли баённомаси билан тасдиққа тавсия этилган (Кафедра мудири, доцент П.З.Давронов)

Кириш

Ўқитишнинг мақсади ва вазифаси

а)курсининг мақсади: талабаларга компьютер тизимларининг ахборот хафсизлиги ва ҳимоя қилишни тамойилларини; Windows операцион тизимини ва унинг иловаларида паролли ҳимоялашни; асосий ташкилий, техникавий ва дастурий воситаларидан фойдаланишни; компьютер вирусида ва уларни қарши воситалар билан таъминлашни; Internetда ахборотларни ҳимоя қилишни ўргатиш.

б) курснинг вазифалари: талабаларда компьютер тармоқлари ва тизимларида ахборот ҳавфсизлиги тўғрисида билимларни шакллантириш; ахборотни ҳимоя қилишнинг назарий, амалий ва услубий асосларини бериш; компьютер тармоқлари ва тизимларида ахборот хавфсизлигини таъминлашнинг замонавий усуллари ва воситаларини қўллашни ўргатиш; талабаларни ахборотларни ҳимоя қилиш бўйича ишлаб чиқилган турли хил дастурий маҳсулотлардан эркин фойдалана олиш имконини берадиган билимлар билан таъминлаш.

Фан бўйича талабаларнинг билимига ўқувига ва кўникмасига қўйиладиган талаблар

а) тасаввурга эга бўлмоғи лозим: ахборотнинг жисмоний бутунлигини таъминлашни, ахборотни тегишли ҳуқуқларга эга бўлмаган шахслар ёки жараёнлар орқали тармоқдан рухсат этилмаган ҳолда олишга йўл қўймаслик; эгаси тамонидан берилаётган (сотилаётган) ахборот ва ресруслар фақат тамонлар ўртасида келишилган шартлар асосида қўлланилишиши;

б) билиши керак: компьютер тармоқлари ва тизимларидаги ахборот хавфсизлигига таҳдид солиши кутилаётган хавф -хатарнинг моҳиятини ва оқибатларини; компьютер тармоқлари ва тизимларида ахборотни ҳимоя қилиш бўйича қўйиладиган асосий талаблар ва асосларни; ахборотни ҳимоя қилишда қўлланиладиган замонавий амалий тизимлар ва дастурий махсулотларни ишлатишни;

в) бажариши лозим: ҳимоя қилишнинг ишончли тизимини қуриш; турли хил вазифали ва турли хил тегишли ахборотларни умумий берилганлар базасига мужассамлаштириш; рухсат этилмаган мурожаат қилишни; берилганларни нусхалаш ва алмаштириш; ахборотларни шифрлаш усулларини.

Ўқув режасидаги бошқа фанлар билан алоқаси

"Компьютер тизимларида ахборотларни ҳимоялаш" фани "Ахборот технологиялари", "Информатика", "Олий математика" фанлари билан чукур алоқада бўлади.

Фанни ўқитишдаги янги технологиялар

"Компьютер тизимларида ахборотларни ҳимоялаш" фанининг ўқитиш энг замонавий илғор ахборот ва компьютер технологияси ютуқлари асосида олиб борилади.

Фаннинг мазмуни

Кириш. Ахборотларга нисбатан мавжуд хавф-хатарлар асослари

Ахборотларга нисбатан мавжуд хавфсизликларнинг асосий тушунчалари ва унинг таснифи. Ахборот хавфсизлигига кириш. Предметнинг асосий тушунчалари ва мақсади. Ахборотларга нисбатан хавф-хатарлар таснифи. Тармоқ хавфсизлигини назорат қилиш техник воситалари

Автоматлаштирилган ахборот тизимларида маълумотларга нисбатан хавфлар. Автоматлаштирилган ахборот тизимларида ҳимоялаш зарурияти. Ахборотни ҳимоялаш тизими.Ташкилотлардаги ахборотларни ҳимоялаш. Ҳимоялаш тизимининг комплекслиги. Ахборотларни ташкилий ҳимоялаш элементлари. Ахборот тизимларида маълумотларга нисбатан хавф-хатарлар

Вирус ва антивируслар таснифи. Вирус ва унинг турлари. Зарарланган диск. Компьютер вируси. Компьютер вирусларидан ахборотларга рухсатсиз кириш ва улардан фойдаланишни ташкил этиш. Антивирус дастурлари. Вирусларга қарши чора- тадбирлар

Замонавий компьютер стенографияси ва криптографияси

Ахборотларни стенографик ҳимоялаш усуллари. Замонавий компьютер стенографияси.Компьютер стенографияси истиқболлари.Компьютер стенографиясининг асосий вазифалари. Конфидециал ахборотларни киришдан ҳимоялаш. Мониторинг ва тармоқ захираларини бошқариш тизимларини

енгиш. Дастурий таъминотни ниқоблаш. Муаллифлик ҳуқуқларини ҳимоялаш.Стенографик дастурлар тўғрисида қисқача маълумот

Ахборотларни крептографик ҳимоялаш усуллари. Крептография ҳақида асосий тушунчалар. Кодлаштириш ва шифрлаш. Ахбротларни криптографияли ҳимоялаш тамойиллари. Компьютер маълумотларини ҳимоялашнинг техник-дастурий воситалари. Симметрияли криптотизим асослари.Ўринларни алмаштириш усуллари. Алмаштириш усуллари

Компьютер тармоқларида маълумотларнинг рухсатсиз тарқалиши ва уларни бартараф этиш усуллари

Маълумотларни тарқалиб кетиши ва маълумотларга рухсатсиз кириш Ахборот тизимларининг таъсирчан қисмлари. Электрон почтага рухсатсиз кириш.Маълумотларга рухсатсиз киришнинг дастурий ва техник воситалари

Компьютер тармоқларида маълумотларни тарқалиш каналлари

Компьютер тармокларининг заиф қисмлари. Тармоқ ҳимоясининг ташкил этиш асослари. Компьютер телефониясидаги ҳимоялаш усуллари

Компьютер тармоқларида замонавий ҳимоялаш усуллари ва воситалари

Компьютер тармоқларида ҳимояни таъминлаш усуллари. ЭҲМ ҳимоясини таъминлашнинг техник воситалари. Компьютер тармоқларида маълумотларни ҳимоялашнинг асосий йўналишлари. Internet тармоғида мавжуд алоқанинг ҳимоясини таъминлаш асослари

Internet тизимида маълумотлар хавфсизлигини таъминлаш усуллари ва воситалари

Internetда ахборотлар хавфсизлигини таъминлаш асослари. Internet га рухсатсиз кириш усулларининг таснифи. Рухсат этилган манзилларнинг рухсат этилмаган вақтда уланиши. Тармоқлараро экран ва унинг вазифалари.Тармоклараро экраннинг асосий компонентлари

Электрон почтада ахборотларга нисбатан мавжуд хавф-хатарлар ва улардан ҳимояланиш асослари. Электрон почтадан фойдаланиш. E-mail асослари. E-mail даги мавжуд муаммолар. Электрон почтада мавжуд хавфлар.Электрон почтани ҳимоялаш.

Электрон тўловлар тизимида ахборотларни ҳимоялаш. Электрон тўловлар тизими асослари. Идентификацияловчи шахсий номерни ҳимоялаш. POS тизими хавфсизлигини таъминлаш.Банкоматлар хавфсизлигини таъминлаш.Internet да мавжуд электрон тўловлар хавфсизлигини таъминлаш.Ахборотларни ҳимоялашнинг асосий воситалари

Компьютер тизимларининг ҳимояланганлик даражасини аниқлаш воситалари.Асосий тушунчалар.Sustem Security Scanner (SSS) дастури хақида.SATAN ва Internet Scanner SAFE дастурлари

Амалий ва лаборатория машғулотлари

Windows операцион тизимини паролли ҳимоялаш

Операцион тизимларни паролли ҳимоялаш. Паролларни ўрнатиш ва олиб ташлаш

Windows операцион тизимида файл ва, папкалар тузиш, нусхаларини яратиш ва архивлаш

Windows XP папка ва файллар яратиш. Папка ва файллар нусхаларини яратиш. Архиватор дастурлари.Windows XP папка ва файлларни архивлаш. Архивланган папка ва файлларни очиш.

Windows XP иловалари паролли ҳимоялаш

Microsoft Word XP дастурида файллар тузиш ва уларга парол ўрнатиш. Microsoft Excel XP дастурида файллар тузиш ва уларга парол ўрнатиш.

Антивирус дастурлари

Антивирус дастурлари ҳакида. NOD32 антивирус дастури унинг имкониятлари. Касперского Personal антивирус дастури ва унинг имкониятлари. Антивирус дастурлари билан ишлаш.

Ахборотларни стенографик ҳимоялаш усуллари Ахборотларни шифрлашда ўринларни алмаштириш усули.

Ахборотларни ўринларни алмаштириш усули билан шифрлаш. Ахборотларни таянч сўзли ўринларни алмаштириш усули билан шифрлаш

Ахборотларни стенографик ҳимоялаш усуллари

Ахборотларни шифрлашни Цезар усули. Ахборотларни Цезар усули билан шифрлаш. Ахборотларни аффин тизимидаги Цезар усули билан шифрлаш. Таянч сўзли Цезар усули

Ахборотларни гаммалаш усули билан шифрлаш

Таққосламалар ҳакида асосий тушунчалар. Ахборотларни гаммалаш усули билан шифрлаш

Ахборотларни симметрик усул билан шифрлаш. Вижинер усули. Ахборотларни Вижинер жадвали билан оддий шифрлаш усули. Ахборотларни Вижинер жадвали билан калитли шифрлаш.

Ахборотларни криптографик ҳимоялашни аналитик усуллари. Хилл усули. Ахборотларни шифрлашнинг Хилл усули.

Интернетда ахборот хавфсизлиги.

Интенетга рухсатсиз кириш усуллари. Рухсат этилган мазилларнинг рухсат этилмаган вактда уланиши. Тармокларараро экран ва унинг вазифалари. Интернетда ишлаш.

Мустакил таълим мавзулари

Ахборотларни стенографик ҳимоялаш усуллари. Ахборотларни шифрлашни Цезар усули

Ахборотларни Цезар усули билан шифрлаш. Ахборотларни аффин тизимидаги Цезар усули билан шифрлаш.

Ахборотларни симметрик усул билан шифрлаш. Вижинер усули

Ахборотларни Вижинер жадвали билан шифрлаш. Ахборотларни Вижинер жадвали билан калитли шифрлаш

Ахборотларни криптографик ҳимоялашни аналитик усуллари. Хилл усули

Вирусларнинг файллар таркибига таъсири

Файллар таркибини бузувчи ва бузмайдиган вируслар. Оператор ва қурилмаларга таъсир қилувчи вируслар

Ташкилотларда ахборотларни ҳимоялаш

Ташкилотларда ахборотларни ҳимоялаш. Ахборотларни ташкилий ҳимоялаш элементлари. Ахборот тизимларида маълумотларга нисбатан хавф-хатарлар

Электрон тўловлар тизимида ахборотларни ҳимоялаш

Электрон тўловлар тизими. Идентификация шахсий номерини ҳимоялаш. Банкоматлар хавфсизлигини таъминлаш. Интернетда мавжуд электрон туловлар хавфсизлини таъминлаш. Ахборотларни ҳимоялаш воситалари

Компьютер тизимларининг ҳимояланганлик даражасини аниқлаш воситалари

SSS –System security Scanner дастури ва унинг асосий вазифалари. Satan ва Internet Scanner SAFE дастури ва унинг вазифалари.Internet Scanner SAFFEsuite дастури ҳақида

Дарслик ва ўқув қўлланмалар рўйхати

Асосий

1. Алимов Р.Х, Ходиев Б.Ю., Алимов Қ. А., Усмонов С.У., Бегалов Б.Б., Зайналов Н.Р., Мусалиев А.А., Файзиева Ф. Миллий иқтисодда ахборот тизимлари ва технологиялари. «Шарқ» нашриёт-матбаа акциядорлик компанияси бош таҳририяти. Тошкент -2004.

2. Герасименко В.А. Защита информации в автоматизированных системах обработки данных. Москва: 1998

3. Камилов Ш.М., Машарипов А.К., Закирова Т.А., Эрматов Ш.Т., Мусаева М.А. Компьютер тизимларида ахборотни ҳимоялаш. Маъруза матнлари. ТДИУ Тошкент , 2003

4. Р.В.Хамидуллин, И.А.Бригаднов, А.В.Морозов. Методы и средства защиты компьютерной информации. Учебное пособие. Санкт – Петербург. 2005. 87 стр.

5. В.И.Завгродный. Комплексная защита информации в компьютерных системах. Учебное пособие. Москва, Логос; ПБОЮЛ. 2001. 264 стр.

6. Ю.А.Гатчина, А.Г.Коробойников. Основы криптографических алгоритмов. Учебное пособие. Санкт – Петербург. 2002, 29 стр.

Қўшимча

7. М.Г.Адигеев. Ведение в криптографии. Методические указания для студентов механико-математического факультета. Часть 1. Основные понятия, задачи и методы криптографии. Ростов – на – Дону. 2002.

8. Шаньгин В.Ф. «Зищита информации и информационная безопасноть» 2 часть. Москва: «МИЭТ», 2000

9. Интернет ахборот ресурслари; www.ziyonet.uz ва бошк.

II.Компьютер тизимларида ахборотларни химоялаш фанидан

ИШЧИ ЎҚУВ ДАСТУРИ

Ишчи ўқув дастури:
Самарқанд қишлоқ хўжалик институти ўқув ишлари проректори томонидан (29. 08. 2008 й.) тасдиқланган (Проф. Т.Э.Остонақулов)

Ишчи ўқув дастури 30.08. 2006 й. тасдиқланган фан дастурига асосан тузилди.

5340100- "Иқтисодиёт (қишлоқ хўжалиги)" ва 5610100 -"Фермер хўжаликларини бошқариш" бакалавриат таълим йўналиши ўқув дастури, ўқув режаси ва фан дастурига мувофиқ ишлаб чиқилди.

Тузувчилар: доцент Х .Урдушев, доцент М.Рахимов

Тақризчилар: Самарқанд давлат университети

доценти Б.И.Усманов,"Олий математика ва ахборот технологиялари" кафедраси доценти И.Абруев

Ишчи ўқув дастури:

Самарқанд қишлоқ хўжалик институтининг

«Иқтисодиёт ва бошқарув» факултети Илмий кенгашининг 2008 йил 28.08.№1-сон мажлисида муҳокама этилди ва тасдиқланди (Илмий кенгаш раиси доц. А.И.Аликулов).

«Иқтисодиёт ва бошқарув» факултети Услубий кенгашининг 2008 йил 27.08.№1-сон мажлисида муҳокама этилди ва тасдиқланди (Услубий кенгаш раиси доц. Р.Усмонов).

«Олий математика ва ахборот технологиялари» кафедрасининг 2008 йил 26 августдаги №1-сон мажлис қарори билан тасдиқланди (Кафедра мудири доц. П.Давронов)

Дарс соатлари тақсимоти: 18 соат маъруза, 18 соат лаборатория (18 соат амалий машғулот ФХБ йўналиши учун) ва 28 соат мустақил таълим)

II.1.Маъруза машғулотларининг мавзулари

Мавзу №.	Маъруза №	Мавзулар мазмуни	Соат
1-мавзу. Ахборотларга нисбатан мавжуд хавф-хатарлар асослари (6 соат). Адабиёт: 1-16			
	1-маъруза	1.1.Ахборотларга нисбатан мавжуд хавфсизликларнинг асосий тушунчалари ва унинг таснифи	2
	2-маъруза	1.2. Автоматлаштирилган ахборот тизимларида маълумотларга нисбатан хавфлар	2
	3-маъруза	1.3.Вирус ва антивируслар таснифи	2
2-мавзу. Замонавий компьютер стенографияси ва криптографияси (4соат). Адабиёт: 1-14			
	4-маъруза	2.1.Ахборотларни стенографик ҳимоялаш усуллари	2
	5-маъруза	2.2.Ахборотларни крептографик ҳимоялаш усуллари	2
3-мавзу. Компьютер тармоқларида маълумотларнинг рухсатсиз тарқалиши ва уларни бартараф этиш усуллари (4соат). Адабиёт: 1-19			
	6-маъруза	3.1.Маълумотларни тарқалиб кетиши ва маълумотларга рухсатсиз кириш 3.2.Компьютер тармоқларида маълумотларни тарқалиш каналлари	2
	7-маъруза	3.3.Компьютер тармоқларида замонавий ҳимоялаш усуллари ва воситалари	2
4-мавзу. Internet тизимида маълумотлар хавфсизлигини таъминлаш усуллари ва воситалари (4 соат). Адабиёт: 1-14			
	8-маъруза	4.1.Internetда ахборотлар хавфсизлигини таъминлаш асослари 4.2.Электрон почтада ахборотларга нисбатан мавжуд хавф-хатарлар ва улардан ҳимояланиш асослари	2
	9-маъруза	4.3.Электрон тўловлар тизимида ахборотларни ҳимоялаш 4.4. Компьютер тизимларининг ҳимояланганлик даражасини аниқлаш воситалари	2

II.2.Амалий машғулот ва лаборатория ишлари мавзулари

Т.р.	Мавзулар номи ва мазмуни	Режа
1	**Мавзу. Windows операцион тизимини паролли ҳимоялаш** 1.Операцион тизимларни паролли ҳимоялаш 2.Паролларни ўрнатиш ва олиб ташлаш **Лаборатория иши № 1** (Макс. 4 балл). Ад.4	2
2	**Мавзу. Windows операцион тизимида файл ва, папкалар тузиш, нусхаларини яратиш ва архивлаш** 1.Windows XP папка ва файллар яратиш 2.Папка ва файллар нусхаларини яратиш 3.Архиватор дастурлари. 4.Windows XP папка ва файлларни архивлаш. 5.Архивланган папка ва файлни очиш. **Лаборатория иши № 2** (Максимал 4 балл) Ад.4	
3	**Мавзу. Windows XP иловалари паролли ҳимоялаш** 1.Microsoft Word XP дастурида файллар тузиш ва уларга парол ўрнатиш. 2.Microsoft Excel XP дастурида файллар тузиш ва уларга парол ўрнатиш. 3.Компьютерда вазифалар бажариш **Лаборатория иши № 3** (Максимал 4 балл). Ад.4	2
4	**Мавзу. Антивирус дастурлари** 1.Антивирус дастурлари ҳақида 2.NOD32 антивирус дастури унинг имкониятлари. 3.Касперского Personal антивирус дастури ва унинг имкониятлари 4.Антивирус дастурлари билан ишлаш **Лаборатория иши № 4** (Максимал 4 балл). Ад.4	
5	**Мавзу. Ахборотларни стенографик ҳимоялаш усуллари Ахборотларни шифрлашда ўринларни алмаштириш усули** 1.Ахборотларни ўринларни алмаштириш усули билан шифрлаш. 2.Ахборотларни таянч сўзли ўринларни алмаштириш усули билан шифрлаш **Лаборатория иши № 5** (Максимал 4 балл). Ад.4	2
6	**Мавзу. Ахборотларни стенографик ҳимоялаш усуллари. Ахборотларни шифрлашни Цезар усули** 1.Ахборотларни Цезар усули билан шифрлаш 2.Ахборотларни аффин тизимидаги Цезар усули шифрлаш. 3.Таянч сўзли Цезар усули **Лаборатория иши № 6** (Максимал 4 балл). Ад.4	2
7	**Мавзу. Ахборотларни гаммалаш усули билан шифрлаш** 1.Тақкосламалар ҳақида асосий тушунчалар 2.Ахборотларни гаммалаш усули билан шифрлаш **Лаборатория иши № 7** (Макс. 4 балл). Ад.4	4

Т.р.	Мавзулар номи ва мазмуни	Режа
8	**Мавзу. Ахборотларни симметрик усул билан шифрлаш. Вижинер усули** 1.Ахборотларни Вижинер жадвали билан оддий шифрлаш усули. 2.Ахборотларни Вижинер жадвали билан калитли шифрлаш **Лаборатория иши № 8** (Макс. 4 балл) Ад.4	2
9	**Мавзу. Ахборотларни криптографик ҳимоялашни аналитик усуллари. Хилл усули.** Ахборотларни шифрлашнинг Хилл усули **Лаборатория иши № 9** (Макс. 4 балл) Ад.4	4
	Жами	18

II.3.Мустақил таълим мавзулари

	Мустақил таълим мавзулари ва мазмуни	Соат
	Назарий қисм бўйича (Мавзуларда тегишли вазифалар бажарилади)	
1	**Ахборотларни стенографик ҳимоялаш усуллари. Ахборотларни шифрлашни Цезар усули.** Ахборотларни Цезар усули билан шифрлаш. Ахборотларни аффин тизимидаги Цезар усули билан шифрлаш. Ад.4	4
2	**Ахборотларни симметрик усул билан шифрлаш. Вижинер усули.** Ахборотларни Вижинер жадвали билан оддий шифрлаш. Ахборотларни Вижинер жадвали билан калитли шифрлаш . Ад.4	4
3	**Ахборотларни криптографик ҳимоялашни аналитик усуллари. Хилл усули.** Ад.4	4
	Амалий қисм бўйича	
4	**Вирусларнинг файллар таркибига таъсири.** Файллар таркибини бузувчи ва бузмайдиган вируслар. Оператор ва қурилмаларга таъсир қилувчи вируслар Ад.1-19	4
5	**Ташкилотларда ахборотларни ҳимоялаш.** Ташкилотларда ахборотларни ҳимоялаш. Ахборотларни ташкилий ҳимоялаш элементлари. Ахборот тизимларида маълумотларга нисбатан хавф-хатарлар. Ад.1-19	4
6	**Электрон тўловлар тизимида ахборотларни ҳимоялаш** Электрон тўловлар тизими. Идентификация шахсий номерини ҳимоялаш. Банкоматлар хавфсизлигини таъминлаш. Интернетда мавжуд электрон туловлар хавфсизлини таъминлаш. Ад.1-19	4
7	**Компьютер тизимларининг ҳимояланганлик даражасини аниқлаш воситалари.** SSS –System security Scanner дастури ва унинг асосий вазифалари. Satan ва Internet Scanner SAFE дастури ва унинг вазифалари.Internet Scanner SAFFEsuite дастури ҳақида. Ад.1-19	4
	Жами	28

II.4 «Компьютер тизимида ахборотларни ҳимоялаш» фанидан якуний баҳолаш саволлари

Ахборотларга нисбатан мавжуд хавф-хатарлар асослари.Ахборотларга нисбатан мавжуд хавфсизликларнинг асосий тушунчалари ва унинг таснифи

1. Ахборот хавфсизлигига кириш
2. Предметнинг асосий тушунчалари ва мақсади
3. Ахборотларга нисбатан хавф-хатарлар таснифи
4. Тармоқ хавфсизлигини назорат қилиш техник воситалари
5. Операцион тизим иловаларига ҳимоя ўрнатиш

Автоматлаштирилган ахборот тизимларида маълумотларга нисбатан хавфлар

6. Автоматлаштирилган ахборот тизимларида ҳимоялаш зарурияти
7. Ахборотни ҳимоялаш тизими
8. Ташкилотлардаги ахборотларни ҳимоялаш.
9. Ҳимоялаш тизимининг комплекслиги.
10. Ахборотларни ташкилий ҳимоялаш элементлари
11. Ахборот тизимларида маълумотларга нисбатан хавф-хатарлар

Вирус ва антивируслар таснифи

12. Вирус ва унинг турлари.
13. Зарарланган диск.
14. Компьютер вируси.
15. Компьютер вирусларидан ахборотларга рухсатсиз кириш ва улардан фойдаланишни ташкил этиш.
16. Антивирус дастурлари.
17. Вирусларга қарши чора- тадбирлар

Замонавий компьютер стенографияси ва криптографияси.Ахборотларни стенографик ҳимоялаш усуллари

18. Замонавий компьютер стенографияси
19. Компьютер стенографияси истиқболлари
20. Компьютер стенографиясининг асосий вазифалари
21. Конфидециал ахборотларни киришдан ҳимоялаш.
22. Мониторинг ва тармоқ захираларини бошқариш тизимларини енгиш.
23. Дастурий таъминотни ниқоблаш.
24. Муаллифлик ҳуқуқларини ҳимоялаш.
25. Стенографик дастурлар тўғрисида қисқача маълумот.

Ахборотларни крептографик ҳимоялаш усуллари

26. Крептография ҳақида асосий тушунчалар.
27. Кодлаштириш ва шифрлаш.
28. Ахбротларни криптографияли ҳимоялаш тамойиллари
29. Компьютер маълумотларини ҳимоялашнинг техник-дастурий воситалари.
30. Симметрияли криптотизим асослари.
31. Ўринларни алмаштириш усуллари
32. Алмаштириш усуллари

Компьютер тармоқларида маълумотларнинг рухсатсиз тарқалиши ва уларни бартараф этиш усуллари.

33. Ахборот тизимларининг таъсирчан қисмлари
34. Электрон почтага рухсатсиз кириш
35. Маълумотларга рухсатсиз киришнинг дастурий ва техник воситалари

Компьютер тармоқларида маълумотларни тарқалиш каналлари

36. Компьютер тармоқларининг заиф қисмлари.
37. Тармоқ ҳимоясининг ташкил этиш асослари.
38. Компьютер телефониясидаги ҳимоялаш усуллари

Компьютер тармоқларида замонавий ҳимоялаш усуллари ва воситалари

39. Компьютер тармоқларида ҳимояни таъминлаш усуллари
40. ЭҲМ ҳимоясини таъминлашнинг техник воситалари
41. Компьютер тармоқларида маълумотларни ҳимоялашнинг асосий йўналишлари
42. Internet тармоғида мавжуд алоқанинг ҳимоясини таъминлаш асослари.

II.5.Фан бўйича адабиётлар рўйхати ва интернет ахборот ресурсларидаги электрон версияларининг номи

1. Алимов Р.Х, Ходиев Б.Ю., Алимов Қ. А., Усмонов С.У., Бегалов Б.Б., Зайналов Н.Р., Мусалиев А.А., Файзиева Ф. Миллий иқтисодда ахборот тизимлари ва технологиялари. «Шарқ» нашриёт-матбаа акциядорлик компанияси бош таҳририяти. Тошкент -2004.

2. Герасименко В.А. «Защита информации в автоматизированных системах обработки данных» Москва: 1998

3. Камилов Ш.М., Машарипов А.К., Закирова Т.А., Эрматов Ш.Т., Мусаева М.А. Компьютер тизимларида ахборотни ҳимоялаш. Маъруза матнлари. ТДИУ Тошкент , 2003

4. Ҳ.Урдушев, М.Рахимов. Компьютер тизимларида ахборотларни ҳимоялаш фанидан амалий, лаборатория иши ва мустақил таълим вазифаларини бажариш учун услубий қўлланма.СамҚХИ. Самарқанд 2007 йил.

Интернетдан олинган электрон версиялар:

5. В.И.Завгородный. Комплексная защита информации в компьютерных системах. Учебное пособие. Москва. "Логос". 2001. 264 с.

6. В.А.Голуб. Парольная зашита. Учебно - методическое пособие. ВГУ. Воронеж. 2005.

7. Р.Р.Хамидулина, И.А.Бригаднов, А.В.Морозов. Методы и средство зашиты компьютерной информации. Учебное пособие. СЗТУ. Санкт - Петербург. 2005. 178 с.

8. В.Н.Будко. Информационная безопасность и зашита информации (Конспект лекций). ВГУ. Воронеж. 2003. 86 с.

9. М.Г.Адигеев. Введение в криптографию. Методические указания. Часть 1. Ростовский ГУ. Ростов-на-дону. 2002. 35 с.

10.Ю.А. Гатчин, А. Г.Коробейников. Основы криптографических алгоритмов. Учебное пособие. ИТМО (Технический университет). СПб. 2002. 29 с.

11. А.В.Терехов, В.Н.Чернышов, А.В.Селезнев, И.П.Рак. Зашита компьютерной информации. Учебное пособое. Томбов. Изд-во ТГТУ.2003 г. 80 с.

12. В.А.Голуб.Система контроля доступа. Учебно-методическое пособие. ВГУ. Воронеж. 2004. 15 с.

13.Брюс Шнайер. Прикладная криптография. 2-е издание. Протоколы, алгоритмы и исходные тексты на языке С. 2001

14. Ю.В.Романец. П.А.Тимофеев, В.Ф.Шаньгин. Защита информации в компьютерных системах и сетях. Под ред. В.Ф.Шаньгина. "Радио и связь"Москва. 2001. 376 с.

15.11.С.Г.Баричев, Р.Е.Серов. Основы современной криптографии. Ver 1.3. 151с.

16.С.Баричев. Криптография без секретов. Книга. Интернет.

17. Г.Г.Елинова. Информационные технологиии в профессиональной деятельности. Краткий курс лекци.Оренбург. ОГУ. 2004. 39 с.

18. В.В.Ященко - Введение в Криптографию.271 с

19. К.В.Ржавский. Информационная безопасность – практическая защита информационных технологий и телекоммуникационных систем. Учебное пособие. ВолГУ. 2002. 122с.

II.6.Фан бўйича талабаларни баҳолаш тартиби

1.Маъруза машғулотлари бўйича:

1) Фан бўйича талабаларни оралиқ баҳолашга 45 балл ажратилиб, унинг 15бали мустақил таълимга ажратилган.Қолган 30 бални тўплаш учун 1-маротаба оралиқ назорат ўтказилади;

2) Мустақил таълим бўйича 15 балл оралиқ баҳолаш балларини олиш учун талаба «Мустақил таълим мавзулари режаси» да келтирилаётган 1-3 мавзуларини (бу ерда ҳар бир мавзу - максимал 5 балдан баҳоланади) бажариб, белгиланган тартибда расмийлаштириб, маъруза ўқийдиган профессор - ўқитувчига топширади.

- **1-оралиқ баҳолаш ∑ = 30 балл; 2-оралиқ баҳолаш ∑= 15 балл.**

Амалий ва лаборатория машғулотлари бўйича:

1) Фан бўйича талабаларни жорий баҳолашга 40 балл ажратилиб, унинг 4 бали мустақил таълимдан тўпланади. Қолган 36 балл эса 9 та лаборатория ишларини бажариш натижасига кўра баҳоланади. Ҳар бир лаборатория иши - максимал 4 балл билан баҳоланади.

2) Мустақил таълим бўйича 4 балл жорий баҳолаш балини тўплаш учун талаба «Мустақил таълим мавзулари режаси» да келтирилаётган 4-7 мавзуларини бажариб, белгиланган тартибда расмийлаштириб амалий машғулот ўтадиган профессор - ўқитувчига топширади;

3) Ўрганиладиган мавзулар сони ва ҳажмини амалиёт ўқитувчиси талабанинг фанни билиши, ўзлаштириш даражаси, дарсларда фаол қатнашишига кўра белгилайди.

- **1-жорий баҳолаш ∑= (Лаб.№1+Лаб.№2+Лаб.№3) = 12 балл;**
- **2-жорий баҳолаш ∑= (Лаб.№4+ Лаб.№5+Лаб.№6) = 12 балл;**
- **3-жорий баҳолаш ∑= (Лаб.№7+Лаб.№8+Лаб.№9+ Муст.иш) = 16 балл.**

3. Мустақил таълим ва лаборатория ишларини расмийлаштириш ва топшириш:**1) Реферат форматида А4 форматли қоғозда; 2) Реферат форматида умумий дафтарда; 3) Компьютерда бажарилган рефератнинг электрон версияси шаклида.**

Баҳолаш тури	Юқори балл	Баҳолаш мезонлари			
		0 – 54 балл	55 – 70 балл	71 – 85 балл	86 – 100 балл
Оралиқ баҳолаш	45	0-24,3	24,8-31,5	32,0-38,3	38,7-45,0
Шундан аудиторияда:					
1-Оралиқ баҳолаш	30	0-16,2	16,5-21	21,3-25,5	25,8-30,0
Мустақил таълимда					
2-Оралиқ баҳолаш	15	0- 8,1	8,3-10,5	10,6-12,8	12,9-15,0
2-Оралиқ баҳолаш	40	21,6	22,0-28,0	28,4-34,0	34,4-40,0
Шундан аудиторияда:					
1-жорий баҳолаш	12	0-6,5	6,6-8,4	8,5-10,2	10,3-12,0
1-жорий баҳолаш	12	0-6,5	6,6-8,4	8,5-10,2	10,3-12,0
1-жорий баҳолаш	16	0-8,7	8,8-11,3	11,4-13,6	13,8-16,0
(1 та лаборатория учун)	(4)	0-2,2	2,3-2.8	2.9-3,4	3.5-4,0
Якуний баҳолаш	15	0- 8,1	8,3-10,5	10,6-12,8	12,9-15,0
Умумий балл	100	0-54	55-70	71-85	86-100

1. Мавзу. Windows операцион тизимини паролли ҳимоялаш

1. Операцион тизимларни паролли ҳимоялаш
2. Паролларни ўрнатиш ва олиб ташлаш

I.**Дарснинг мақсади.** Талабаларга операцион тизимларни паролли ҳимоялаш, паролларни ўрнатиш ва олиб ташлаш усулларини ўргатиш.
II. Информацион техник ва услубий воситалар
II.1. Pentium компьютерлари, кадоскоп, видеоплеер ва плакатлар
II.2. Адабиётлар: [1, 2, 3, 4, 5, 6, 7] ва мавзу бўйича тарқатма материаллар

1.1.Операцион тизимларни паролли ҳимоялаш

Паролли ҳимоялашга тўхталамиз.

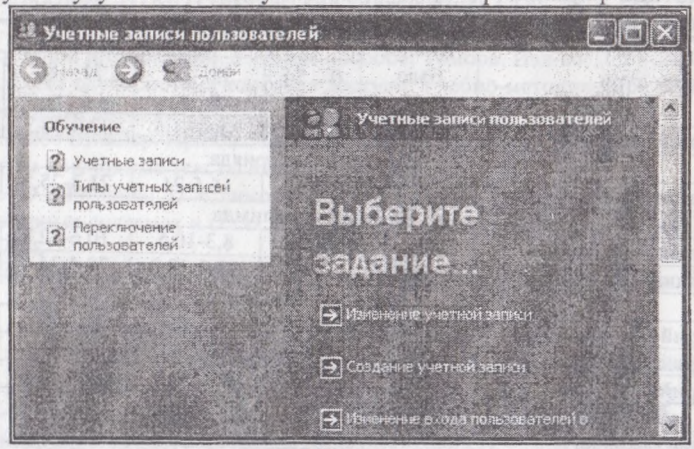
1.**Windows XP** да парол ўрнатиш учун **Пуск ▸ Настройка ▸ Панель управления** буйруқларини берамиз. Натижада монитор экранига **Панель управления** (Бошқариш панели) диалог ойнаси чиқарилади.

2. Бу ойнадаги файллар рўйхатидан (Фойдаланувчиларнинг ҳисобини ёзиш)ни фаоллаштириб, контекст менюдан **Открыть** буйруғи берилади.

3. Ойнага чиқариладиган **Учетные записи пользователей** мулоқот ойнасининг **Выберите задание** (Вазифани танланг) бандида қуйидагилар келтирилади: **Изменение учетной записи** (Ҳисобга олиш ёзувларни ўзгартириш); **Создание учетной записи** (Ҳисобга олиш ёзувларни тузиш); **Изменение входа пользователей в систему** (Системага кирувчи фойдаланувчиларни ўзгартириш).

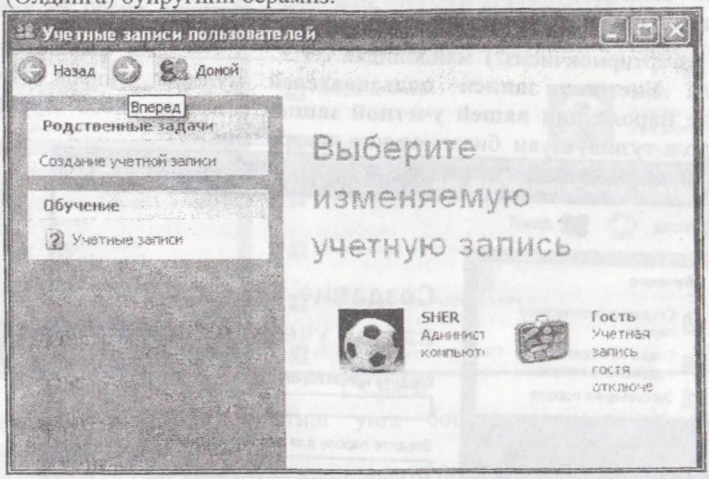
Юқорида келтирилганлардан **Изменение учетной записи** нинг функцияларини қараб чиқайлик.

4. Бунинг учун **Изменение учетной записи** ни фаоллаштирамиз.

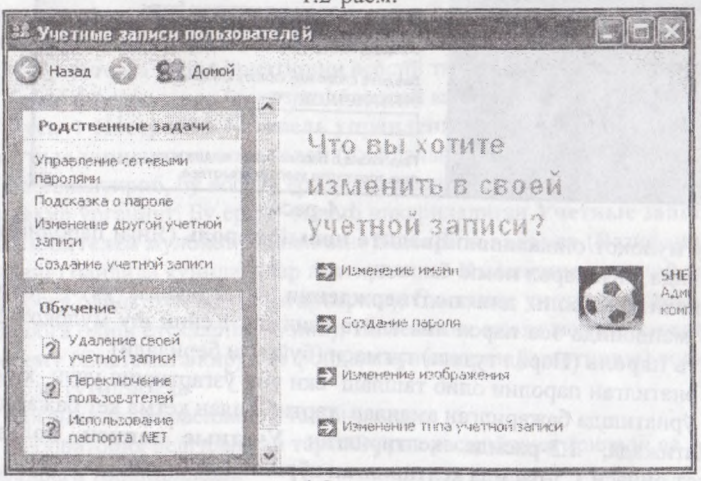


1.1-расм.

Натижада 1.1-расмда келтирилган мулокот ойнаси 1.2-расмдаги кўринишни олади. Бу ойнадаги **Выберите изменяемую учетную запись** (Ўзгартириладиган ёзувни танланг) майдонидан SHER ни танлаймиз ёки **Вперед** (Олдинга) буйруғини берамиз.



1.2-расм.

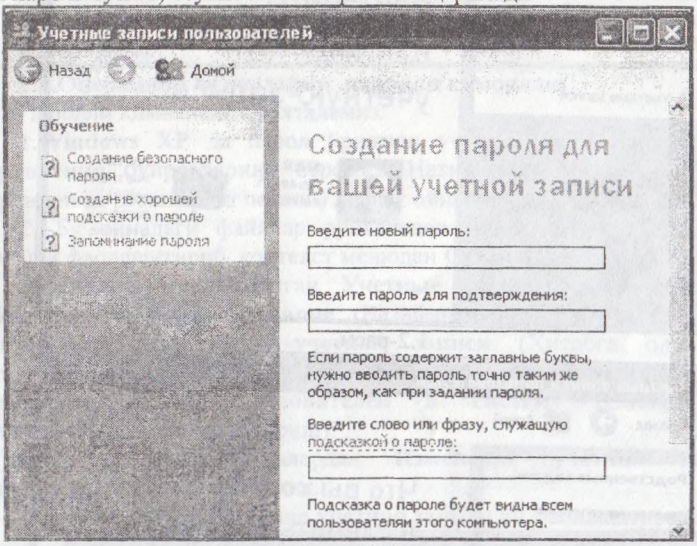


1.3-расм.

Натижада **Учетные записи пользователей** мулокот ойнаси 1.3-расмда келтирилган кўринишни олади. Бу мулокот ойнасида куйидаги вазифаларни бажариш мумкин: **Изменение имени** (Қўйилган номни ўзгартириш); **Создания пароля** (Парол тузиш); **Изменения изображения** (Тасвирни ўзгартириш); **Измениния типа учетной записи** (Ҳисобга олиш ёзувларини типини ўзгартириш); **Использовать паспорт .NET** (.NET паспортини қўллаш).

1.2. Паролларни ўрнатиш ва олиб ташлаш

Демак, биз операцион тизимга кириш учун парол қўймоқчи бўлсак, **Учетные записи пользователей** мулоқот ойнасининг **Что вы хотите изменить в своей учетной записи?** (Сиз ўзингизнинг ҳисоб ёзувингиздан нимани ўзгартирмоқчисиз?) майдонидан Создание пароля ни фаоллаштирамиз. Натижада **Учетные записи пользователей** мулоқот ойнаси (1.4-расм) **Создание пароля для вашей учетной записи** (Сизнинг ҳисоб ёзувларингиз учун пароль тузиш) ёзуви билан экранга чиқарилади.



1.4-расм.

Бу мулоқот ойнасининг **Введите новый пароль** (Янги паролни киритинг) майдонида янги парол номи ёзилади.

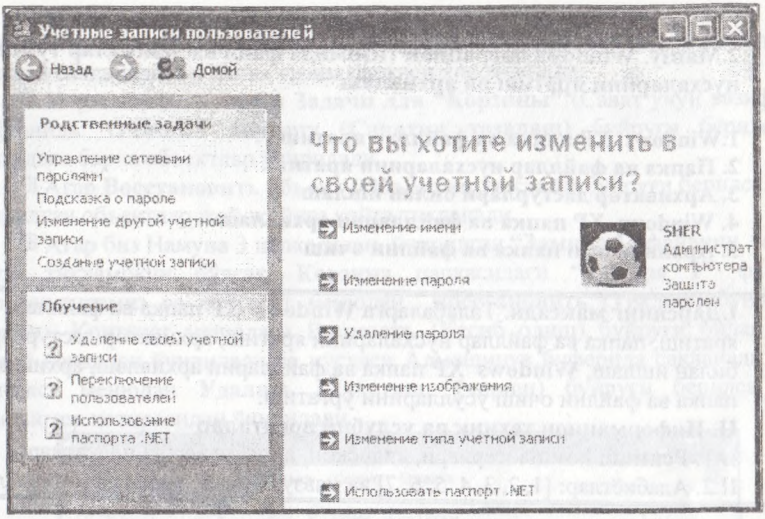
Введите пароль для подтверждения (Тасдиклаш учун паролни яна ёзинг) майдонида эса парол яна қайта ёзилади. Кейин шу мулоқот ойнасидан **Создать пароль** (Парол тузиш) тугмаси (буйруғи берилади)

Ўрнатилган паролни олиб ташлаш ёки уни ўзгартириш учун ҳам юқорида парол ўрнатишда бажарилган амаллар тартиб билан кетма кет бажарилади.

Натижада, 1.3-расмда келтирилган **Учетные записи пользователей** мулоқот ойнаси 1.5-расмда келтирилган кўринишни олади.

Бу ойнадаги **Изменение пароля** (Паролни ўзгартириш) воситаси ёрдамида ўрнатилган парол ўзгартириса, **Удаления пароля** (Паролни олиб ташлаш) билан ўрнатилган парол олиб ташланади.

Сиз компьютерга парол ўрнатиш бўйича малака ва кўникма ҳосил қилишингиз учун юқорида келтирилганларни амалда бажариб кўришингиз лозим бўлади.



1.5-расм.

Компьютерга парол ўрнатиш унга бошқа кишиларнинг рухсатсиз киришидан ҳимоялайди.

Компьютерга бир нечта пароллар ўрнатилиши мумкин. Бу ерда бир нечта фойдаланувчилар назарда тутилмоқда.

Мавзу бўйича лаборатория ишини расмийлаштириш тартиби:

1) Компьютерга парол ўрнатишни асосий таснифларини келтиринг;
2) Компьютерга парол ўрнатишни асосий вазифаларини таснифланг;
3) **Пуск ▸ Настройка ▸ Панель управления** буйрукларини беринг **Учетные записи пользователей** (Фойдаланувчиларнинг ҳисобини ёзиш) ни фаоллаштириб, бу восита ёрдамида амалга ошириладиган ишларни мустақил ўрганинг. Бу ерда: ойнага чиқариладиган **Учетные записи пользователей** мулоқот ойнасининг **Выберите задание** (Вазифани танланг) бандида қуйидагилар келтирилади: **Изменение учетной записи** (Ҳисобга олиш ёзувларни ўзгартириш); **Создание учетной записи** (Ҳисобга олиш ёзувларни тузиш); **Изменение входа пользователей в систему** (Системага кирувчи фойдаланувчиларни ўзгартириш) воситалари назарда тутилмоқда
4) Ўрганилган жараёнларни таснифланг.
5) Лаборатория белгиланган тартибларда расмийлаштирилади ва кафедрага топширилади.
6) Лабораториянинг электрон версияси ҳам қабул қилинади.

2.Мавзу. Windows операцион тизимида файл ва папкалар тузиш, нусхаларини яратиш ва архивлаш

1.Windows XP папка ва файллар яратиш
2. Папка ва файллар нусхаларини яратиш
3. Архиватор дастурлари билан ишлаш
4. Windows XP папка ва файлларни архивлаш
5. Архивланган папка ва файлни очиш

I.Дарснинг мақсади. Талабаларга **Windows XP** папка ва файллар яратиш, папка ва файллар нусхаларини яратиш, архиватор дастурлари билан ишлаш, **Windows XP** папка ва файлларни архивлаш, архивланган папка ва файлни очиш усулларини ўргатиш.
II. Информацион техник ва услубий воситалар
II.1. **Pentium** компьютерлари, кадоскоп, видеоплеер ва плакатлар
II.2. Адабиётлар: [1, 2, 3, 4, 5, 6, 7] ва мавзу бўйича тарқатма материаллар

2.1.Windows XP папка ва файллар яратиш

1.Компьютерда **Windows** операцион тизимини юкланг.

2.**Рабочий стол** (Иш столи)да **Намуна 3** номли папка яратинг. Бунинг учун иш столининг бўш жойида контекст менюнини очинг ва ундан **Создать ▸ Папку** буйруғини беринг. Ҳосил бўлган папкани Намуна 3 номда расмийлаштиринг

3.Иш столидаги объект, файл ва пакаларни нусхасини Намуна 3 папкасида яратинг. Бунинг учун иш столидаги бирорта файлини фаоллаштиринг ва контекст менюдан **Копировать** (Нусха олиш) буйруғини беринг. Кейин Намуна 3 папкасини фаоллаштиринг ва контекст менюдан **Вставить** (Олинган нусхани қўйиш) буйруғини беринг. Бу ишни бошқа бир нечта файл ва объектлар учун бажаринг.

4. Намуна 3 папкасидаги файл ва папкаларни қайта бошқа ном билан расмийлаштиринг. Бунинг учун папкадаги файлни фаоллаштиринг ва контекст менюдан **Переименовать** (Қайта номлаш) буйруғини беринг ва файлнинг номлар майдончасида исмингизни, масалан **"Замира 1"** ни ёзиб клавиатурадан **Enter** тугмасини босинг. Бу ишни бошқа файллар учун бажаринг. Файлларни мос равишда **"Замира 2","Замира 3"** ва ҳ.к. янги номлар билан расмийлаштиринг.

5. Янги файлларни архиватор дастурлар ёрдамида архив нусхаларини яратинг. Архивланадиган файлларга пароль ўрнатинг. Ўрнатилган пароллар номини эслаб қолинг.

6. Намуна 3 папкасидаги **"Замира 2"** файлини фаоллаштиринг ва контекст менюдан **Удалить** (Йўқотиш, ўчириш) буйруғини беринг. Бу ишни қолган файллар учун такрорланг.

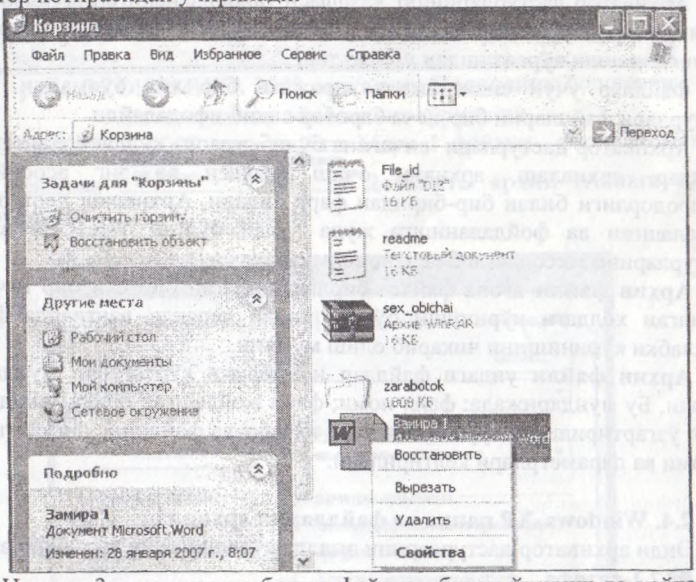
7. Иш столидан **Корзина** (Сават) папкасини очинг. Бунинг учун **Корзина** папкасини фаоллаштириб, контекст менюдан **Открыть** (Очиш) буйруғини

беринг. **Корзина (Савat)** папкасида ўчирилган файллар, объектлар ва папкалар рўйхати сақланади. Бу папка тизим папкаси ҳисобланади.

Корзина папкасидаги **Задачи для "Корзины"** (Савat учун вазифалар) майдонида: **Очистить корзину (Саватни тозалаш)** буйруғи берилса бу папкадаги барча объектлар ўчирилади.

Агар **Восстановить объект (Объектни тиклаш)** буйруғи берилса барча ўчирилган объектлар жой-жойига қайта тикланади.

Агар биз Намуна 3 папкасидан ўчирилган **"Замира 1"** файлини жойига қайта тикламоқчи бўлсак, **Корзина** папкасидаги **"Замира 1"** файлини фаоллаштирамиз ва контекст менюдан **Восстановить** (Тиклаш) буйруғини берамиз. Контекст менюдаги **Вырезать** (Кесиб олиш) буйруғи билан файл жорий папкадан ўчирилади ва нусхаси Алмашинув буферида сақланади. Агар контекст менюдан **Удалить** (Йўқотиш, ўчириш) буйруғи берилса файл компьютер хотирасидан ўчирилади.



Намуна 3 папкасидаги бошқа файллар билан ўчириш ва қайта тиклаш амалларини бажаринг. Мавзу бўйича кўникма ва малака ҳосил қилинг.

2.2. Папка ва файллар нусхаларини яратиш

Операцион тизим фойдаланувчига папка ва файлларнинг нусхасини яратиш кўплаб усулларини таклиф қилади, масалан:

Файл фаоллаштирилади;

1) «Сичқонча» ўнг тугмаси босилиб чиқариладиган контекст менюдан **Создать** буйруғи берилади;
2) Дастур жорий файли, масалан **Документ 1** (матн муҳаририда) ёки **Книга 1** (электрон жадвалда) ном билан тузади.

3) Фойдаланувчи янги ном билан файлни тегишли папка ёки ахборот ташувчи воситаларда ёзиб қўйиши мумкин;
4) Ҳужжатни нусхасини **Файл** менюсининг **Сохранить как** буйруғи билан ҳам яратиш мумкин. Бундай ҳолларда файлга тегишли папка ёки ахборот ташувчи воситаларда ёзиб қуйиш ёки бошқа ном берилади.
5) Нусхалашни Контекст менюдан Копировать буйруғи билан ҳам амалга ошириш мумкин. Кейин файл нусхаси тегишли папка ёки ахборот ташувчи воситаларда ёзиб қўйилади.

2.3. Архиватор дастурлари

Архивлаш дастурлари – компьютер дискида жойни тежаш мақсадида файллар ҳажмини кичрайтиришга имкон берувчи дастурдир.[1] Улар турлича кўринишда ишлатилса ҳам, ишлаш тамойили бир хил: файлларда айнан такрорланадиган ўринлар мавжуд бўлиб, уларни дискда сақлаш мазмунсиз ҳисобланади.

Архиватор дастурларининг вазифаси такрорланадиган шундай бўлакларни топиб, уларни ўрнига бошқа бирор маълумотни ёзиш ҳамда уларнинг кетма-кетлигини аниқ кўрсатишдан иборатдир.

Файллар учун сиқилганлик даражаси бир хил бўлмайди. Архивлаш дастурлари файлларни бир-неча баробар сиқиб ифодалайди.

Архиватор дастурлари анчагина бўлиб, уларда қўлланиладиган математик усуллар, архивлаш, архивни очиш тезлиги ва энг асосийси, сиқиш самародорлиги билан бир-биридан фарқ қилади. Архивлаш дастурларига анча оммалашган ва фойдаланишга жуда қулай бўлган **WinRAR** ва **WinZIP** дастурларини мисол қилиб келтириш мумкин.

Архив файли ягона файлга бирлаштирилган бир ёки бир неча файлнинг сиқилган ҳолдаги кўриниши бўлиб, ундан керакли вақтларда файлларнинг дастлабки кўринишини чиқариб олиш мумкин.

Архив файли ундаги файллар номларини кўрсатувчи мундарижага эга бўлади. Бу мундарижада: файл номи; файл жойлашган папка ҳақида маълумот; файл ўзгартирилгани кўрсатувчи сана ва вақт ва файлнинг дискдаги, архивдаги ўлчами ва параметрлари келтирилади.

2.4. Windows XP папка ва файлларни архивлаш

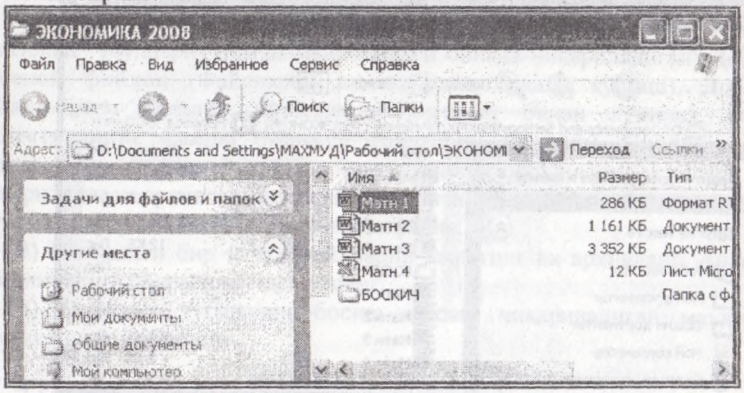
Энди архиватор дастурларини амалда қўлланишини кўриб чиқайлик.

2.1-вазифа.

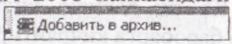
1. Windows операцион тизимини юкланг.
2. Windows иш столини фаоллаштиринг ва унда ЭКОНОМИКА 2008 номли янги папка тузинг.
3. ЭКОНОМИКА 2008 папкасига иш столидаги файл ёки объектларини нусхаларини жойлаштиринг. Жойлаштирилган файлларни **Матн1, Матн 2, Матн 3, ...** янги номлар билан қайта расмийлаштиринг.
4. ЭКОНОМИКА 2008 папкасини **Проводник** (Бошловчи) билан фаоллаштиринг (очинг). Бу папка ичида БОСҚИЧ номли янги папка тузинг ва

[1] А.А.Абдукодиров ва бошқ. Ахборот технологиялари.Тошкент. Ўқитувчи.2002.

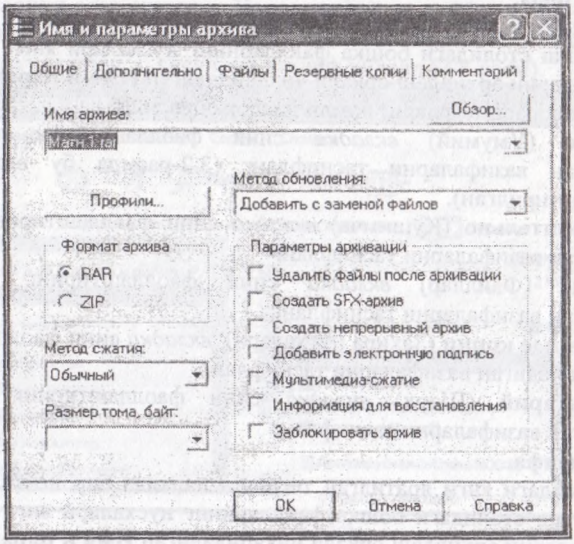
унга ҳам иш столидаги файлларнинг нусхаларини жойлаштиринг ва уларни ҳам бошқа янги номлар билан, масалан **Сардор1, Сардор 2, Сардор 3, ...** билан расмийлаштиринг.



2.1-расм. ЭКОНОМИКА 2008 папкасини **Проводник** бошловчи билан очилган ойнасининг кўриниши.

5. ЭКОНОМИКА 2008 папкасидаги Матн 1 файлни фаоллаштиринг ва контекст менюдан 

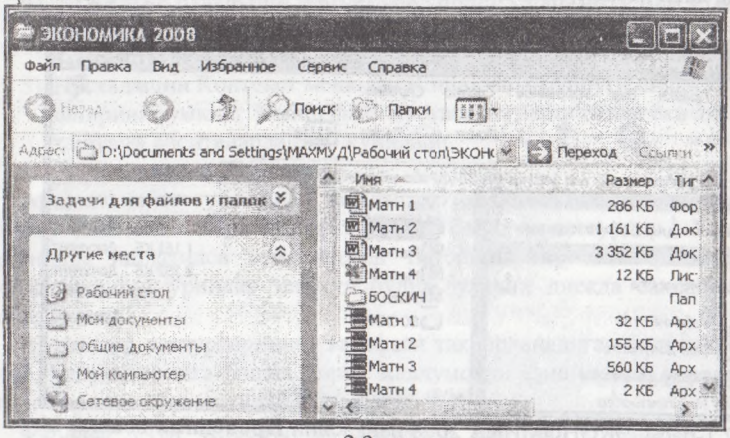
Добавить архив (Ахивга қўшиш) буйруғини беринг.



2.2-расм.

Натижада монитор ойнасида **Имя и параметры архива** номли диалог ойнаси чиқарилади. Бу ойнадан **ОК** тугмасини босинг. Бу ишни қолган

файллар учун ҳам бажаринг. Архивланган файлларни кўриниши 2.3-расмда келтирилган.



2.3-расм.

Биз қараётган мисолда (2.3-расм) Матн 3 файлининг ўлчами 3352 Кб бўлса, бу файл архивлангач ўлчами 560 Кб ни ташкил килган. Демак, файлни архивлаш натижасида унинг ўлчами 6 баробарга кичрайтирилган (сиқилган).

Амалий ва лаборатория иши топшириқлари.

2.2-вазифа.

Иш столидаги янги яратилган тегишли папкада бир нечта янги файллар яратинг ёки иш столидаги бошқа файлларнинг нусхалари янги номлар билан тузинг. Файлларни архивлаш орқали чиқариладиган **Имя и параметры архива** (Архив ном ива параметрлари) номли диалог ойнасида:

1)**Общие** (Умумий) *вкладка* сини фаоллаштиринг ва у билан бажариладиган вазифаларни таснифланг (3.2-расмда бу вкладкани фаол кўриниши келтирилган).

2)**Дополнительно** (Қўшимча) *вкладка* сини фаоллаштиринг ва у билан бажариладиган вазифаларни таснифланг

3)**Файлы** (Файллар) *вкладка* сини фаоллаштиринг ва у билан бажариладиган вазифаларни таснифланг.

4)**Резервные копии** (Захира нусхалари) *вкладка* сини фаоллаштиринг ва у билан бажариладиган вазифаларни таснифланг.

5)**Коментарий** (Шарҳ) *вкладка* сини фаоллаштиринг ва у билан бажариладиган вазифаларни таснифланг

2.3-вазифа.

Иш столидаги янги яратилган тегишли папкада бир нечта янги файллар яратинг ёки иш столидаги бошқа файлларнинг нусхалари янги номлар билан тузинг. Файлларни архивлаш орқали чиқариладиган **Имя и параметры архива** номли диалог ойнасида:

1)**Общие** *вкладка* сини фаоллаштиринг ва унинг **Метод сжатия** (Сиқиш усуллари) номли майдонидаги ойнада чиқариладиган: **Без сжатия** (Сиқишсиз),

Скоростной (Тезкор), **Быстрый** (Тезда), **Хороший** (Яхши), **Максимальний** (Максимал) усуллари билан бажариладиган архивлашларни бирорта файл мисолида ўрганинг. Уларни умумий ва фарқли томонларини таснифланг.

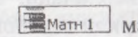
2)**Общие** *вкладка* сини фаоллаштиринг ва унинг **Метод обновления** (Янгилаш усуллари) номли майдонидаги ойнада чиқариладиган: **Добавить с заменой файлов** (Файлларни алмаштириш орқали қўшиш), **Добавить с обнавлением файлов** (Файлларни янгилаш билан қўшиш), **Обновить существуюшие файлы** (Мавжуд файлларни янгилаш), **Синхронизировать содержимое файлов** (Файллар мазмунини синхронлаш) усуллари билан бажариладиган архивлаш ишларини бирорта файл мисолида ўрганинг. Уларни умумий ва фарқли томонларини таснифланг.

3) Папкадаги бир нечта файлларни ажратинг ва архивланг. Архивланган файлни очинг. Жараённи таснифланг.

4) **Справка** тугмасини босиш орқали чиқариладиган маълумотнома тизимидан фойдаланинг.

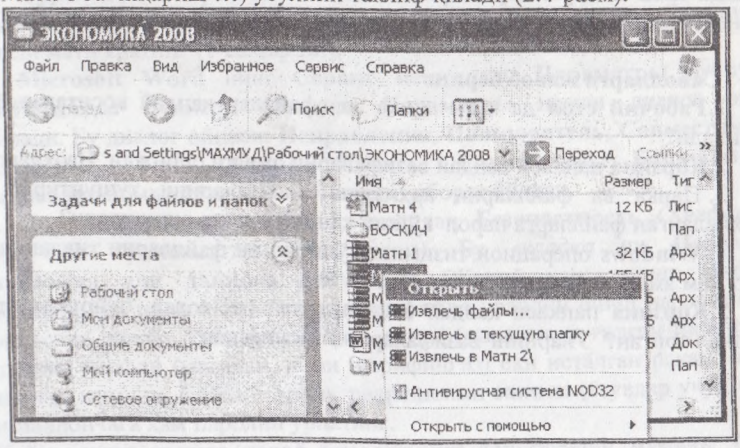
2.5. Архивланган папка ва файлни очиш

Архивланган папка ва файлларни очиш вазифалар бажариш орқали ўрганамиз.

1.Папкадаги архивланган файлни, масалан архивланган 

матн 1 файлини фаоллаштирамиз.

2.Архивланган матн фаоллаштириб чиқариладиган контекст менюдан, архив файлларини очишни учта: **Извлечь файлы …**(Файлларни чиқариш…) , **Извлечь в текущую папку…**(Жорий папкага чиқариш…), **Извлечь в Матн 1…** (Матн 1 га чиқариш …) усулини таклиф қилади (2.4-расм).



2.4-расм.

Амалий ва лаборатория иши топшириқлари

2.4-вазифа.

1)ЭКОНОМИКА 2008 папкасидаги Матн 1архивланган файлни фаоллаштиринг ва контекст менюдан **Извлечь файлы** …(Файлларни чиқариш…) буйруғини беринг. Бажарилган ишларни таснифланг.

2)ЭКОНОМИКА 2008 папкасидаги Матн 2 архивланган файлни фаоллаштиринг ва контекст менюдан **Извлечь в текущую папку**…(Жорий папкага чиқариш…) буйруғини беринг. Бажарилган ишларни таснифланг.

3)ЭКОНОМИКА 2008 папкасидаги Матн 3 архивланган файлни фаоллаштиринг ва контекст менюдан **Извлечь в Матн 1…** (Матн 1 га чиқариш …) буйруғини беринг. Бажарилган ишларни таснифланг.

4)ЭКОНОМИКА 2008 папкасидаги БОСҚИЧ архивланган папкани фаоллаштиринг ва контекст менюдан **Извлечь в Матн 1…** (Матн 1 га чиқариш …) буйруғини беринг. Бажарилган ишларни таснифланг.

Лаборатория ишини бажариш учун кўрсатмалар

Мавзу бўйича 2.1-2.3 вазифаларни умумлаштириб лаборатория иши тайёрланади. Лаборатория ишида архвлаш усуллари, уларнинг умумий ва фаркли томонлари таснифланади.

Кўрсатма.

Мавзуни ўрганишда ва лаборатория ишида архивлашнинг таснифларини ёзишда **Имя и параметры архива** диалог ойнасидаги **Справка** тугмасини босиш орқали чиқариладиган маълумотнома матнларидан фойдаланинг.

Саволларга жавоб беринг

1.**Рабочий стол** да янги папка ва файллар қандай воситалар ёрдамида тузилади?

2.**Корзина** папкаси қандай вазифаларни амалга оширади. Изоҳланг.

3. Папка ва файлларни архивлаш воситаларини тушунтириб беринг. Архивланган файлларга парол қўйиш қандай амалга оширилади?

4. **Windows** операцион тизимида ўчирилган файлларни тиклашни ҳамма вақт ҳам амалга ошириш мумкинми?

5.**Корзина** папкаси қандай воситалардан (менюлар, буйруқлар тўплами) ташкил топган? Уларнинг вазифаларини таснифланг.

3.Мавзу. Windows XP иловалари паролли ҳимоялаш

3.1. **Microsoft Word XP** дастурида файллар тузиш ва уларга парол ўрнатиш
3.2. **Microsoft Excel XP** дастурида файллар тузиш ва уларга парол ўрнатиш
3.3. Компьютерда вазифалар бажариш

I.Дарснинг мақсади. Талабаларга **Microsoft Word XP** ва **Microsoft Excel XP** дастурида файллар тузиш ва уларга парол ўрнатишни ўргатиш.
II. Информацион техник ва услубий воситалар
II.1. Pentium компьютерлари, кадоскоп, видеоплеер ва плакатлар
II.2. Адабиётлар: [1, 2, 3, 4, 5, 6, 7] ва мавзу бўйича тарқатма материал

3.1. Microsoft Word XP дастурида файллар тузиш ва уларга парол ўрнатиш

1.Компьютерда **Windows** операцион тизимини юкланг.

2.**Рабочий стол** (Иш столи)да **Намуна 4** номли папка яратинг. Бунинг учун иш столининг бўш жойида контекст менюни очинг ва ундан **Создать ▸ Папку** буйруғини беринг. Ҳосил бўлган папкани **Намуна 4** номда расмийлаштиринг

3. **Намуна 4** номли папкасида контекст менюдан **Создать ▸ Документ Microsoft Word** буйруғини беринг. Янги тузилган **Microsoft Word** ҳужжатини Намуна 4 папкасида, ўз номингиз билан (масалан, "Турсинтош 4") расмийлаштиринг

4. "Турсинтош 4" файлини очинг (юкланг). Бунинг учун, бу файлни фаоллаштириб контекст менюдан **Открыть** (Очиш) буйруғини беринг.

5. "Турсинтош 4" файлида " Худойбердиева Турсунтошнинг иқтисодиёт ва бошқарув факультетида –ўқиш даврида бажараётган ишлари " мавзусида ҳужжатли матн яратинг (1-саҳифали).

6. **Microsoft Word** нинг **Сервис** менюсидан **Параметры** буйруғини беринг.Натижада монитор ойнасига **Параметры** номли диалог ойнаси чиқарилади. Бу диалог ойнаси: **Исправления, Пользователь, Совместимость, Расположение, Вид, Общие, Печать, Сохранение, Безопастность, Правописание** номли 11 та *вкладка* лардан иборат бўлади.

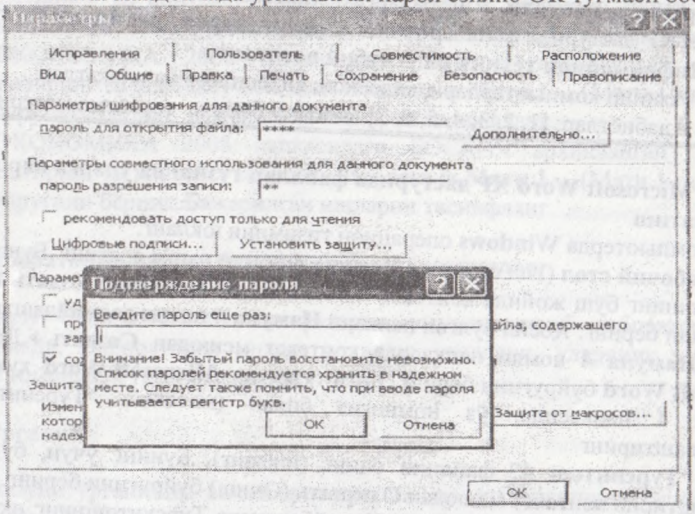
7. **Параметры** номли диалог ойнасидан **Безопастность** (Хавфсизлик) *вкладка* сини фаоллаштиринг (3.1-расм). Бу *вкладка* ни **Параметры шифрования для данного документа** (Жорий ҳужжатнинг шифрлаш параметрлари) да **пароль для открытия файла** (файлни очиш пароли) номли майдончасида пароль ўрнатинг. Парол рақам (масалан, туғилган йилингиз ва санангиз)ли, ҳарфли (масалан, исми шарифингиз) ёки исталган рақам, номлар бўлишингиз мумкин. Кейин **пароль разрешения записи** (ёзувлар учун парол) номли майдончага ҳам паролни ўрнатинг.

Қуйиладиган иккита парол бир хил ёки ҳар бўлиши мумкин. Сўнгра **Параметры** номли диалог ойнасидан **ОК** тугмасини босинг. Натижада **Подтверждение пароля** (Паролни тасдиқлаш) ойнаси чиқарилади. Бу ойнада пароль қайта ёзилиб яна **ОК** тугмаси босилади. (Ҳурматли талаба қўйган паролингизни эслаб қолинг. Пароллар ҳарфли (мантли) бўлса ва қайси

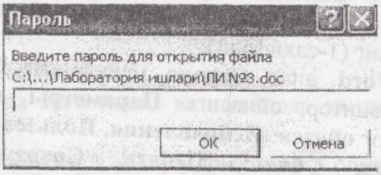
алифбода (масалан, рус алифбоси ёки лотин алифбоси) ўша алифбода ёзилиши шарт)

8.Жорий файлни ёпинг.

9. Жорий (масалан, "Турсинтош 4") файлни қайта юкланг. Натижада монитор экранига **Пароль** номли диалог ойнаси чиқарилади (3.2–расм). Бу ойнадаги тегишли майдончада ўрнатилган парол ёзилиб **ОК** тугмаси босилади.



3.1-Расм.



3.2-Расм

3.1. Вазифа.

Microsoft Word да бир нечта файллар яратинг. Уларга парол ўрнатинг. Парол ўрнатиш жараёнини таснифланг.

3.2. Microsoft Excel XP дастурида файллар тузиш ва уларга парол ўрнатиш

Вазифани бажариш учун кўрсатмалар

1.Компьютерда **Windows** операцион тизимини юкланг.

2.**Рабочий стол** (Иш столи)да **Намуна 5** номли папка яратинг. Бунинг учун иш столининг бўш жойида контекст менюнини очинг ва ундан **Создать ▸ Папку** буйруғини беринг. Ҳосил бўлган папкани **Намуна 5** номда расмийлаштиринг

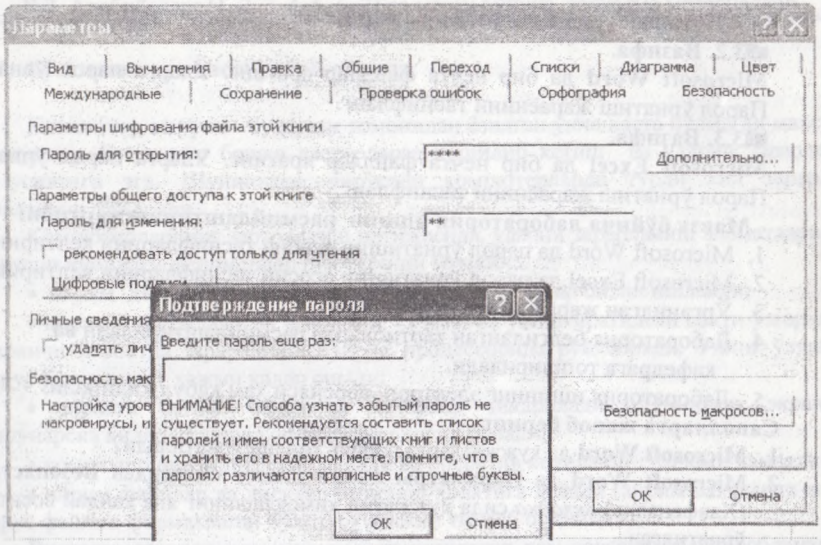
3. **Намуна 5** номли папкасида контекст менюдан **Создать ▸ Лист Microsoft Excel** буйруғини беринг. Янги тузилган **Microsoft Excel** файлини

Намуна 5 папкасида, ўз номингиз билан (масалан, "Олимжон 5") расмийлаштиринг

4. "Олимжон 5" файлини очинг (юкланг). Бунинг учун, бу файлни фаоллаштириб контекст менюдан **Открыть** (Очиш) буйруғини беринг.

5. "Олимжон 5" файлида, масалан "Қишлоқ хўжалиги маҳсулотларини ишлаб чиқаришни иқтисодий кўрсаткичлари"бўйича электрон жадвал яратинг. Ёки исталган иқтисодий мазмуда электрон жадвал тузинг.

6. **Microsoft Excel** нинг **Сервис** менюсидан **Параметры** буйруғини беринг.Натижада монитор ойнасига **Параметры** номли диалог ойнаси чиқарилади. Бу диалог ойнаси: **Вид, Вычисления, Правка, Общие,Списки, Диаграмма, Цвет, Международные, Сохранение, Проверка ошибок, Орфография, Безопастность** номли 13 та *вкладка* лардан иборат бўлади.



3.3-Расм.

7. **Параметры** номли диалог ойнасидан **Безопастность** (Хавфсизлик) *вкладка* сини фаоллаштиринг (3.3-расм). Бу *вкладка* ни **Параметры шифрования для данного книги** (Жорий китобнинг шифрлаш параметрлари) да **пароль для открытия** (очиш учун парол) номли майдончасида парол ўрнатинг. Парол рақам (масалан, туғилган йилингиз ва санангиз) ли, ҳарфли (масалан, исми шарифингиз) ёки исталган рақам, номлар бўлишингиз мумкин.

8. Энди **пароль для изменения** (файлни ўзгартириш) номли майдончага ҳам паролни ўрнатинг.

Қуйиладиган иккита пароль бир хил ёки ҳар бўлиши мумкин.

9.Сўнгра **Параметры** номли диалог ойнасидан **ОК** тугмасини босинг. Натижада **Подтверждение пароля** (Паролни тасдиқлаш) ойнаси чиқарилади. Бу ойнада парол қайта ёзилиб яна **ОК** тугмаси босилади.

Компютер вируслари - инсон томондан ёзилган махсус дастур бўлиб, компютернинг дастурий таъминотини ва унинг тизимли соҳаларини бузиш (бузғунчилик) ишларини амалга ошириш учун мўлжалланган.

Вирусларнинг типик ўлчами ўнлаб байтлардан торитиб то ўнлаб килобайтгача бўлиши мумкин.

Компютер вируслари қўйидаги типларда бўлиши мумкин:

1) **Файлли вируслар.** Улар **exe** ва **com** файлларини, айрим ҳолларда фақат **com** файлларини ишдан чиқаришга мўлжалланган. Бундай вируслар биринчи навбатда буйруқ процессори ва у орқали бошқа барча дастурлар зарараланади. Оператив хотирада доимий қоладиган вируслар энг хавфли вируслар ҳисобланади ва улар резидентли вируслар дейилади.

Вирус билан зарарланган дастурни бир маротаба ишлатишданоқ, зарарланиш жараёни бошланади. Бу ҳолатда вирус бошқариладиган ҳолатга келади ва фаоллашади.

Бундай вируслар дастурлар ва малумотларни бузади, айрим ҳолларда қаттиқ дискдаги барча сақланаётганларни ҳам йўқотиш (ўчириш)и мумкин.

2) **Юкланувчи ёки «бут»ли вируслар.** Бу вируслар қаттиқ ва юмшоқ дискетларни юкланиш секторларини ишдан чиқаради. Улар компютерлар учун жуда хавфли ҳисобланади, чунки уларнинг бузғунчилик ишларининг натижасида компютер юкланишдан тўхташи мумкин, айрим ҳолларда компютерда зарарланган дискетнинг бирор мундарижаси ишлатилгандаёқ, бу жараён рўй бериши мумкин.

3) **Драйверларни зарарловчи вируслар. Бу** вируслар **config.sys** файлида келтирилганларни **DOS**нинг дискли файлларини зарарлайди. Бунинг натижасида компютернинг юкланиши тўхтатилади.

4) DIR вируслари. Бу вируслар файллар таркибини ўзгартиради.

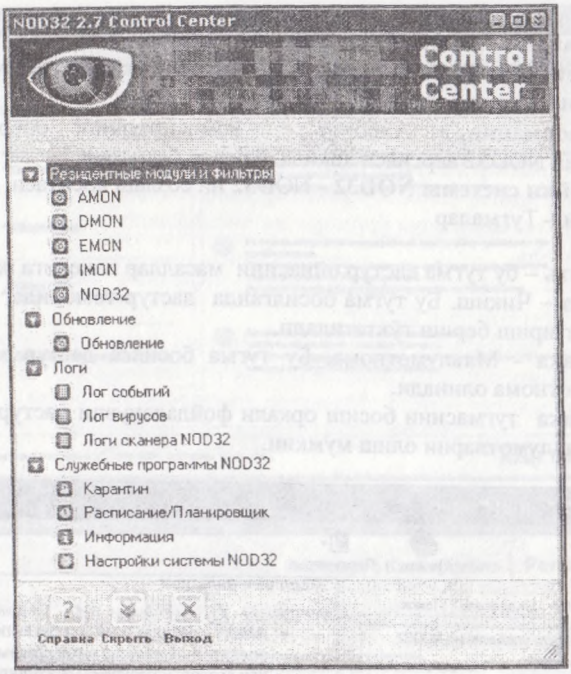
5) **Кўринмас ёки стелс вируслари**. Уларни илғаб ёки пайқаб олиш жуда кийин кечади. Биламизки файл вирус билан зарарланганда, унинг ўлчамлари ошади. Кўринмас вируслар файл ўлчамларини ошишини маскировка қилади яъни фойдаланувчига кўрсатмайди. оддий усулини моҳияти шундаки-файл вирус билан зарарланганда, бу вирус фойдаланувчига гуёҳки, файлнинг ўлчамларини ўзгармаган каби кўрсатади.

6) Ўзи модификацияланувчи вируслар. Улар ўзининг таркибини ва кодини тасодифий қонунга кўра ўзгартириб туради, шу сабабли уларни пайқаш жуда кийин кечади. Уларни яна **полиморф вируслари** деб ҳам аталади. Бир вируснинг икки нусхаси бир хил байтларнинг бир хил кетма-кетлигидан ташкил топмаслиги мумкин.

7) **Тармоқли вируслар.** Бу вируслар тармоқда, шу жумладан **Интернет тизимига** уланиб ишлайдиган компютерларни зарарлайди.

4.2. NOD32 антивирус дастури

Операцион тизимнинг масалалар панелидаги  тугма босилиши билан дастур юкланади ва мониторга **NOD32 2.7 Control Center** диалог ойнаси чиқарилади.



4.1-расм

Бу ойна қуйидаги воситалардан иборат:

Резидентные модули и фильтры (Резидентли модул ва фильтрлар)

- AMON - Сканер на доступе - Сканерга кириш ҳолатида
- DMON - Сканер документов / ActiveX -Ҳужжатларни сканерлаш
- NOD32 - Сканер по требованию -Талабга кўра сканерлаш.
- IMON - Интернет монитор - Интернет монитор
- EMON - Почтовый сканер NOD32 - NOD32 алоқа сканер

Обновление (Янгилаш) – воситаси Интернет орқали барча вирусли компонентларни (вирусли маълумотлар базасини ва бажариладиган модулларни) автоматик янгилаш имкониятини беради.

Зеркало (Ойна) – локал тармоқдаги бошқа ишчи станцияларни янгилаш учун файллар нусхасини яратади.

Логи (Логлар)- тизимли ҳодисалар, вирусли таҳдидларни ва талаб бўйича сканерлашни қўллаб-қувватловчи бошқариш воситаси. Бу ёзувларни фаоллаштирилиши тегишли мурожаатларни фойдаланувчиларга тақдим килади.

- **Лог событий** – ҳодисалар логи;
- **Лог вирусов** – вируслар логи;
- **Лог сканера по требованию** – талаб бўйича сканерлаш логи;
- **Служебные программы NOD32-** NOD32 нинг хизмат дастурлари;
- Бу бўлим қуйидагилардан ташкил топган:

• **Карантин** - карантин папкасини бошқариш;

• **Расписание/Планировщик** –Жадвал/Режалаштирувчи – турли масалаларни режалаштирувчи кучли дастур;

• **Информация** – Ахборот - компьютернинг операцион тизимига ўранатилган NOD32 версияси ҳақида ахборот берилади.

Настройки системы NOD32 - NOD32 ни созлаш воситаси

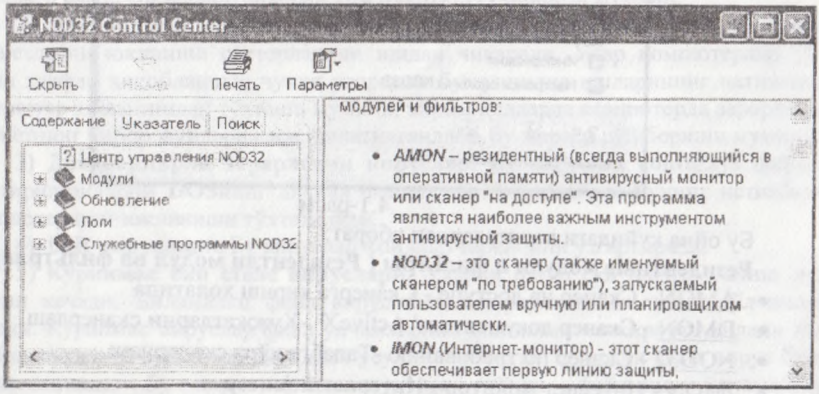
Кнопки – Тугмалар

• **Скрыть** – бу тугма дастур ойнасини масаллар панелига жойлаштиради.

• **Выход** – Чиқиш. Бу тугма босилганда дастур томонидаг вируслар хакида огохлантириш бериш тўхтатилади.

• **Справка** - Маълумотнома. Бу тугма босилса дастур хакида итерактив маълумотнома олинади.

Справка тугмасини босиш орқали фойдаланувчи дастур тўғрисида ўзига керакли маълумотларни олиш мумкин.



4.2-расм.

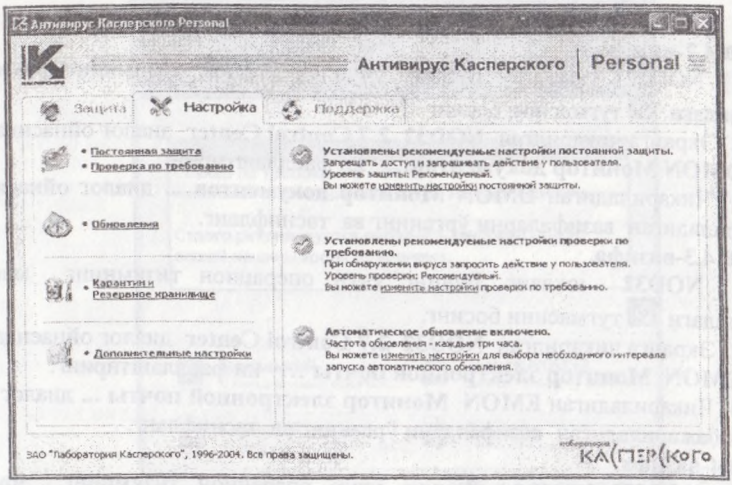
4.3. Касперского Personal антивирус дастури

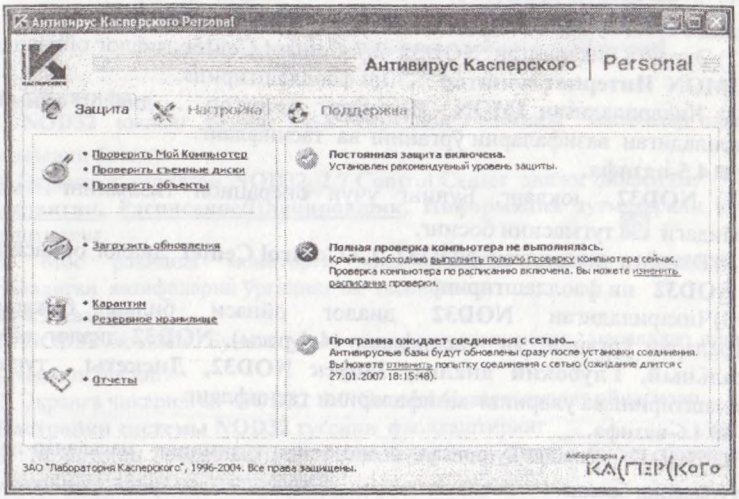
Касперский Персонал антивирус дастури МДҲ давлатларида кенг оммалашган дастурий маҳсулот ҳисобланади.

Антивирус дастурларнинг барчаси умумий таснифларга эга.

Дастурни юклаш унда тегишли вазифаларни бажариш NOD32 каби амалга оширилади. Бу дастур бўйича бошқа маълумотлар мустақил ўрганилади.

Бу восита билан компьютерда ишланади. Қуйидаги расмларда **Антивирус Касперского Personal** дастури ойнасининг кўринишларидан фрагментлар келтирилган.





4.3-расм.

4.4. Антивирус дастурлари билан ишлаш

4.1-вазифа.

1) NOD32 юкланг.Бунинг учун операцион тизимнинг масалалар панелидаги тугмасини босинг.

2) Экранга чиқарилган NOD32 2.7 Control Center диалог ойнасидан **AMON – Сканер по доступу** ни фаоллаштиринг.

3) Чиқариладиган **AMON – Сканер по доступу** диалог ойнаси билан бажариладиган вазифаларни ўрганинг ва таснифланг.

4.2-вазифа.

1) NOD32 юкланг. Бунинг учун операцион тизимнинг масалалар панелидаги  тугмасини босинг.

2) Экранга чиқарилган **NOD32 2.7 Control Center** диалог ойнасидан **DMON Монитор документов…** ни фаоллаштиринг.

3) Чиқариладиган **DMON Монитор документов ...** диалог ойнаси билан бажариладиган вазифаларни ўрганинг ва таснифланг.

4.3-вазифа.

1) **NOD32** юкланг. Бунинг учун операцион тизимнинг масалалар панелидаги  тугмасини босинг.

2) Экранга чиқарилган **NOD32 2.7 Control Center** диалог ойнасидан **EMON Монитор электронной почты …** ни фаоллаштиринг.

3) Чиқариладиган **EMON Монитор электронной почты ...** диалог ойнаси билан бажариладиган вазифаларни ўрганинг ва таснифланг.

4.4-вазифа.

1) **NOD32** юкланг. Бунинг учун операцион тизимнинг масалалар панелидаги  тугмасини босинг.

2) Экранга чиқарилган **NOD32 2.7 Control Center** диалог ойнасидан **IMON Интернет монитор …** ни фаоллаштиринг.

3) Чиқариладиган **IMON Интернет монитор …** диалог ойнаси билан бажариладиган вазифаларни ўрганинг ва таснифланг.

4.5-вазифа.

1) **NOD32** юкланг. Бунинг учун операцион тизимнинг масалалар панелидаги  тугмасини босинг.

2) Экранга чиқарилган **NOD32 2.7 Control Center** диалог ойнасидан **NOD32** ни фаоллаштиринг.

3)Чиқариладиган **NOD32** диалог ойнаси билан бажариладиган вазифаларни ўрганинг ва таснифланг (4.4-расм). **NOD32** диалог ойнасидаги **Локальный, Глубокий анализ, Запуск NOD32, Дискеты** тугмаларини фаоллаштиринг ва уларнинг вазифаларини таснифланг.

4.6-вазифа.

1) **NOD32** юкланг. Бунинг учун операцион тизимнинг масалалар панелидаги  тугмасини босинг.

2) Экранга чиқарилган **NOD32 2.7 Control Center** диалог ойнасидан **Обновление (Янгилаш)** воситасини фаоллаштиринг.

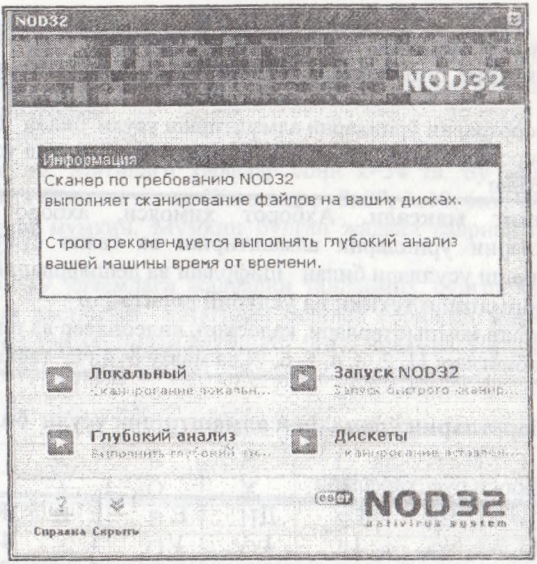
3) Чиқариладиган **Обновление** диалог ойнаси билан бажариладиган вазифаларни ўрганинг ва таснифланг.

4.7-вазифа.

1) **NOD32** юкланг. Бунинг учун операцион тизимнинг масалалар панелидаги  тугмасини босинг.

2) Экранга чиқарилган **NOD32 2.7 Control Center** диалог ойнасидан **Лог событий, Лог вирусов, Лог сканера по требованию** тугмаларини кетма-кет фаоллаштиринг.

3) Мос равишда мониторга чиқариладиган диалог ойналари билан бажариладиган вазифаларни ўрганинг ва таснифланг.



4.4-расм

4.8-вазифа.

1) **NOD32** юкланг. Бунинг учун операцион тизимнинг масалалар панелидаги тугмасини босинг.

2) Экранга чиқарилган **NOD32 2.7 Control Center** диалог ойнасидан **Карантин, Расписание/Планировщик, Информация** тугмаларини кетма-кет фаоллаштиринг.

3) Мос равишда мониторга чиқариладиган диалог ойналари билан бажариладиган вазифаларни ўрганинг ва таснифланг.

4.9-вазифа.

1) **NOD32** юкланг. Бунинг учун операцион тизимнинг масалалар панелидаги тугмасини босинг.

2) Экранга чиқарилган **NOD32 2.7 Control Center** диалог ойнасидан **Настройки системы NOD32** тугсини фаоллаштиринг.

3) Мониторга чиқариладиган **NOD32** диалог ойнаси билан бажариладиган вазифаларни ўрганинг ва таснифланг.

Мавзу бўйича лаборатория ишини расмийлаштириш тартиби:

1) Вирусларнинг асосий таснифлари келтирилади;
2) Антивирус дастурларининг асосий вазифалари таснифланади;
3) Амалий машғулотда ўрганилган 4.1-4.9- вазифалар ўрганилиб антвирус дастурининг умумий таснифи ёритилади. Лаборатория ишида Интернет ахборот ресурсларидан олинган маълумотлардан ҳам фойдаланиш мумкин. Интернетдан олинган маълумотларнинг оригинали лаборатория ишига илова қилинади.
4) Лаборатория белгиланган тартибларда расмийлаштирилади ва кафедрага топширилади.

5.Мавзу. Ахборотларни стенографик ҳимоялаш усуллари Ахборотларни шифрлашда ўринларни алмаштириш усули

5.1. Ахборотларни ўринларни алмаштириш усули билан шифрлаш
5.2. Ахборотларни таянч сўзли ўринларни алмаштириш усули билан шифрлаш

I.Дарснинг мақсади. Ахборот ҳимояси, ахборот хавфсизлигида ахборотларни ўринларни алмаштириш ва таянч сўзли ўринларни алмаштириш усуллари билан шифрлаш ва дешифрлашни ўргатиш.

II. Информацион техник ва услубий воситалар

II.1. Pentium компьютерлари, кадоскоп, видеоплеер ва плакатлар

II.2. Адабиётлар: [1, 2, 3, 4, 5, 6, 7] ва мавзу бўйича тарқатма материал

5.1. Ахборотларни ўринларни алмаштириш усули билан шифрлаш

5.1-жадвал

Кирилл алифбоси рус ҳарфлари

А	Б	В	Г	Д	Е	Ё	Ж	З	И
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
1	2	3	4	5	6	7	8	9	10
Й	К	Л	М	Н	О	П	Р	С	Т
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
11	12	13	14	15	16	17	18	19	20
У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ъ	Ы
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
21	22	23	24	25	26	27	28	29	30
Э	Ю	Я							
↓	↓	↓							
31	32	33							

5.2-жадвал

Кирилл алифбоси ўзбек ҳарфлари

А	Б	В	Г	Д	Е	Ё	Ж	З	И
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
1	2	3	4	5	6	7	8	9	10
Й	К	Л	М	Н	О	П	Р	С	Т
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
11	12	13	14	15	16	17	18	19	20
У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ъ	Э
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
21	22	23	24	25	26	27	28	29	30
Ю	Я	Ў	Қ	Ғ	Ҳ				
↓	↓	↓	↓	↓	↓				
31	32	33	34	35	36				

5.1-вазифа.

$T_{матн}$ ={ОЛИЙ МАТЕМАТИКА ВА АХБОРОТ ТЕХНОЛОГИЯЛАРИ КАФЕДРАСИ АЪЗОЛАРИ} матнини оддий ўринларни алмаштириш усули билан шифрланг.

Бажариш усули. Матндаги ҳарфлар сони к=54 та. Бу жадваллар учун катаклар сони 54 та бўлиши керак. Жадваллар 2x27, 3x18, 6x9, 9x6, 18x3, 27x2 ўлчамларда бўлиши мумкин. Мумкин бўлган жадвал вавриантларини шифр тузувчи танлайди.

1-қадам. Биз 6x9 ўлчамдаги жадвални танлаймиз, сўнгра бу жадвалнинг биринчи устунини дастлабки катагидан бошлаб берилган матн ҳарфларини жадвал катакларига тартиб билан кетма-кет ёзиб чиқамиз. Натижада берилган жадвал қуйидаги кўринишни олади:

О	Т	К	Б	Е	Г	И	Р	З
Л	Е	А	О	Х	И	К	А	О
И	М	В	Р	Н	Я	А	С	Л
Й	А	А	О	О	Л	Ф	И	А
М	Т	А	Т	Л	А	Е	А	Р
А	И	Х	Т	О	Р	Д	Ъ	И

Демак, шифрлаш матни калити 6x9 ўлчамли жадвал бўлади.

2-қадам. Шифрланган матнни тузишда юқоридаги жадвални ҳар бир сатрлари бўйича ҳарфлари олинади: ОТКБЕГИРЗ ЛЕАОХИКАО ИМВРНЯАСЛ ЙААООЛФИА МТАТЛАЕАР АИХТОРДЪИ

Жавоб. $T_{шифрланган\ матн}$ = {ОТКБЕГИРЗ ЛЕАОХИКАО ИМВРНЯАСЛ ЙААООЛФИА МТАТЛАЕАР АИХТОРДЪИ}

5. 2-вазифа.

$T_{шифрланган\ матн}$ = {КАЁМЙУА АРРИДРЛ ДТЛЛАИД РААЛСАА ЛЙШИТМ} матнини оддий ўринларни алмаштириш усули билан дешифрланг. Шифрлаш калити 7x5 ўлчамли жадвал.

Бажариш усули. Шифрлаш калитига кўра 7x5 ўлчамли жадвал тузамиз.

Тузилган жадвалга шифрланган матндаги ҳарфларни сатр бўйича кетма-кет киритамиз:

К	А	Ё	М	Й	У	А
А	Р	Р	И	Д	Р	Л
Д	Т	Л	Л	А	И	Д
Р	А	А	Л	С	А	А
Л	Й	Ш	И	Т	М	

Бу жадвалдаги ҳарфларни сатр бўйича ёзиб, қуйидагиларга эга бўламиз:

КАДРЛ АРТАЙ ЁРЛАШ МИЛЛИ ЙДАСТ УРИАМ АЛДА

Юқоридаги ҳарфлар гуруҳини бирлаштирамиз ва мазмуни бўйича ажратамиз:

КАДРЛАРТАЙЁРЛАШМИЛЛИЙДАСТУРИАМАЛДА

Жавоб. $Т_{\text{дешифрланган матн}}$ = {КАДРЛАР ТАЙЁРЛАШ МИЛЛИЙ ДАСТУРИ АМАЛДА}

5.2. Ахборотларни таянч сўзли ўринларни алмаштириш усули билан шифрлаш

5. 3-вазифа.

$Т_{\text{матн}}$ ={ОЛИЙ МАТЕМАТИКА ВА АХБОРОТ ТЕХНОЛОГИЯЛАРИ КАФЕДРАСИ АЪЗОЛАРИ} матнини КОМПЬЮТЕР таянч сўзи ёрдамида оддий ўринларни алмаштириш усули билан шифрланг.

Эслатма. Шифрлашда олинадиган таянч сўзларини шундай танлаш керакки ундаги бирорта ҳарф яна такрорланмаслиги лозим. Масалан, ТАЛАБАЛАР ни таянч сўз сифатида олиш мумкин эмас. Чунки бу сўзда, А ҳарфи 3 марта , Л ҳарфи эса 2 марта такрорланади.

Вазифанинг бажарилиши.

Матндаги ҳарфлар сони к=54 та. Бу жадваллар учун катаклар сони 54 та бўлиши керак.

1-қадам. Биз юқоридагидек 6х9 ўлчамдаги жадвални танлаймиз, сўнгра бу жадвалнинг биринчи устунини дастлабки катагидан бошлаб берилган матн ҳарфларини жадвал катакларига тартиб билан кетма-кет ёзиб чиқамиз. Натижада берилган жадвал қуйидаги кўринишни олади:

О	Т	К	Б	Е	Г	И	Р	З
Л	Е	А	О	Х	И	К	А	О
И	М	В	Р	Н	Я	А	С	Л
Й	А	А	О	О	Л	Ф	И	А
М	Т	А	Т	Л	А	Е	А	Р
А	И	Х	Т	О	Р	Д	Ъ	И

2-қадам. Бу жадвалга яна иккита сатр қўшиб, биринчи сатр катакларига КОМПЬЮТЕР сўзини жойлаштирамиз, иккинчи сатрга 5.2-жадвал келтирилган ҳарфларнинг мос кодларини ёзиб чиқамиз:

К	О	М	П	Ь	Ю	Т	Е	Р
12	16	14	17	28	31	20	6	18
О	Т	К	Б	Е	Г	И	Р	З
Л	Е	А	О	Х	И	К	А	О
И	М	В	Р	Н	Я	А	С	Л
Й	А	А	О	О	Л	Ф	И	А
М	Т	А	Т	Л	А	Е	А	Р
А	И	Х	Т	О	Р	Д	Ъ	И

3-қадам. Иккинчи сатрдаги сонларни ўсиш тартибида жойлаштирамиз. Сатрдаги ҳарфларнинг ўрни ҳам мос равишда алмаштирилади, яъни:

Е	К	М	О	П	Р	Т	Ь	Ю
6	12	14	16	17	18	20	28	31
→А	В	С	О	И	Н	Д	Т	А
→Р	О	К	Т	Б	З	И	Е	Г
→А	Л	А	Е	О	О	К	Х	И
→С	И	В	М	Р	Л	А	Н	Я
→И	Й	А	А	О	А	Ф	О	Л
→А	М	А	Т	Т	Р	Е	Л	А
→Ъ	А	Х	И	Т	И	Д	О	Р

4-қадам. Шифрланган матнни тузишда юқоридаги жадвалдаги ҳар бир сатрлари бўйича ҳарфлари олинади, яъни: АВСОИНДТА РОКТБЗИЕГ АЛАЕООКХИ СИВМРЛАНЯ ИЙААОАФОЛ АМАТТРЕЛА ЪАХИТИДОР

Жавоб. $Т_{\text{шифрланган матн}}$ = {АВСОИНДТА РОКТБЗИЕГ АЛАЕООКХИ СИВМРЛАНЯ ИЙААОАФОЛ АМАТТРЕЛА ЪАХИТИДОР}

5. 4-вазифа.

$Т_{\text{шифрланган матн}}$ = {ГАТ ИХЕ ЯБХ ЛОН АРО РОЛ ИТО} матнини КОД таянч сўзи ёрдамида ўринларни алмаштириш усули билан шифрланган. Матнни дешифрланг.

Вазифанинг бажарилиши

1-қадам. Даставвал жадвал ўлчамларини аниқлаймиз. ШИФРланган матндаги ҳарфлар сони k = 21 та. КОД таянч сўзи 3 ҳарфдан иборат. Демак, 3x7 ўлчамли жадвал тузамиз:

б) топшириқ

1) {ИНФОРМА} таянч сўзи билан $T_{матн}$ ={ ВЕТЕРИНАРИЯ ВА АГРОНОМИЯ ФАКУЛЬТЕТИ} матнини шифрланг;
2) {ИНФОРМА} таянч сўзи билан шифрланган матнни дешифрланг;
3) Бажарилган ишларни изоҳланг.

5.1.9-вазифа.

а) топшириқ

1) $T_{матн}$ ={КОМЬЮТЕР ТИЗИМЛАРИДА АХБОРОТНИ ҲИМОЯЛАШ ФАНИ} матнини оддий ўринларни алмаштириш усули билан шифрланг
2) Шифрланган матнни дешифрланг;
3) Бажарилган ишларни изоҳланг.

б) топшириқ

1) {БОТИР} таянч сўзи билан $T_{матн}$ ={ВЕТЕРИНАРИЯ ВА АГРОНОМИЯ ФАКУЛЬТЕТИ} матнини шифрланг;
2) {БОТИР} таянч сўзи билан шифрланган матнни дешифрланг;
3) Бажарилган ишларни изоҳланг.

5.1.10-вазифа.

а) топшириқ

1) $T_{матн}$ ={МЕН АХБОРОТЛАРНИ ҲИМОЯЛАШ ФАНИНИ ЯХШИ БИЛАМАН} матнини оддий ўринларни алмаштириш усули билан шифрланг
2) Шифрланган матнни дешифрланг;
3) Бажарилган ишларни изоҳланг.

б) топшириқ

1) {ЁЛҒОНЧИ} таянч сўзи билан $T_{матн}$ ={МЕН АХБОРОТЛАРНИ ҲИМОЯЛАШ ФАНИНИ ЯХШИ БИЛАМАН } матнини шифрланг;
2) {ЁЛҒОНЧИ } таянч сўзи билан шифрланган матнни дешифрланг;
3) Бажарилган ишларни изоҳланг.

5.1.11-вазифа.

а) топшириқ

1) $T_{матн}$ ={МЕН ЖУДА ҲАРАКАТЧАН ТАЛАБАМАНДА} матнини оддий ўринларни алмаштириш усули билан шифрланг
2) Шифрланган матнни дешифрланг;
3) Бажарилган ишларни изоҳланг.

б) топшириқ

1) {ОЛИЙ} таянч сўзи билан $T_{матн}$ ={МЕН ЖУДА ҲАРАКАТЧАН ТАЛАБАМАНДА} матнини шифрланг;
2) {ОЛИЙ} таянч сўзи билан шифрланган матнни дешифрланг;
3) Бажарилган ишларни изоҳланг.

Лаборатория иши вазифалари

I.**Лаборатория ишининг мақсади**. Талабаларда ахборот ҳимояси, ахборот хавфсизлигида ахборотларни ўринларни алмаштириш ва таянч сўзли ўринларни алмаштириш усуллари билан шифрлаш ва дешифрлашни мустақил бажаришни ўргатиш.

II. Информацион техник ва услубий воситалар

II.1. Pentium компьютерлари, кадоскоп, видеоплеер ва плакатлар

II.2. Адабиётлар: [1, 2, 3, 4, 5, 6, 7] ва мавзу бўйича тарқатма материал

5.2.1 -5.2.27 - вариантлар

а) топшириқ

1) $T_{матн}$ ={МЕН .... ИҚТИСОДИЁТ ВА БОШҚАРУВ ФАКУЛЬТЕТИНИНГ ТАЛАБАСИМАН} матнини оддий ўринларни алмаштириш усули билан шифрланг

2) Шифрланган матнни дешифрланг;

3) Бажарилган ишларни изоҳланг.

б) топшириқ

1) {....} таянч сўзи билан $T_{матн}$ ={ МЕН .... ИҚТИСОДИЁТ ВА БОШҚАРУВ ФАКУЛЬТЕТИНИНГ ТАЛАБАСИМАН } матнини шифрланг;

2) {....} таянч сўзи билан шифрланган матнни дешифрланг;

3) Бажарилган ишларни изоҳланг.

1-кўрсатма:

Ҳар бир талаба берилган топшириқ бўйича гуруҳ журналдаги фамилияси исми шарифи бўйича вариант вазифасини тузади.

Масалан, «Иқтисодиёт ва бошқарув» факультети 202- гуруҳ талабаси Аликулова Азизанинг гуруҳ журналидаги тартиб рақами 10 бўлсин. Бу талаба учун вазифа варианти қуйидагича тузилади.

5.2.10 - вариант

а) топшириқ

1) $T_{матн}$ ={МЕН АЛИКУЛОВА АЗИЗА ИҚТИСОДИЁТ ВА БОШҚАРУВ ФАКУЛЬТЕТИНИНГ ТАЛАБАСИМАН} матнини оддий ўринларни алмаштириш усули билан шифрланг

2) Шифрланган матнни дешифрланг;

3) Бажарилган ишларни изоҳланг.

б) топшириқ

1) {....} таянч сўзи билан $T_{матн}$ ={МЕН АЛИКУЛОВА АЗИЗА ИҚТИСОДИЁТ ВА БОШҚАРУВ ФАКУЛЬТЕТИНИНГ ТАЛАБАСИМАН} матнини шифрланг;

2) {....} таянч сўзи билан шифрланган матнни дешифрланг;

3) Бажарилган ишларни изоҳланг.

2-кўрсатма.

1) Шифрлашда жадваллар ўлчами матндаги ҳарфлар сонига қараб аниқланади;

2) Шифрлаш учун таянч сўзини талабанинг ўзи танлайди;

3) Шифрлашда олинадиган таянч сўзларини шундай танлаш керакки ундаги бирорта ҳарф яна такрорланмаслиги лозим.

4) Танланган таянч сўзидаги ҳарфлар сони, жадвал сатридаги катаклар сонига тенг бўлиши лозим.

6. Мавзу. Ахборотларни стенографик ҳимоялаш усуллари. Ахборотларни шифрлашни Цезар усули

6.1. Ахборотларни Цезар усули билан шифрлаш

6.2. Ахборотларни аффин тизимидаги Цезар усули шифрлаш

6.3. Таянч сўзли Цезар усули

I.Дарснинг мақсади. Талабаларга ахборот ҳимояси, ахборот хавфсизлигида ахборотларни Цезар усули, аффин тизимидаги Цезар усули, таянч сўзли Цезар усули билан шифрлаш ва дешифрлаш усулларини қўллашни ўргатиш.

II. Информацион техник ва услубий воситалар

II.1. Pentium компьютерлари, кадоскоп, видеоплеер ва плакатлар

II.2. Адабиётлар: [1, 2, 3, 4, 5, 6, 7] ва мавзу бўйича тарқатма материалллар

6.1. Ахборотларни Цезар усули билан шифрлаш

Бу усулда алмаштирувчи ҳарфлар k та силжитиш орқали амалга оширилади (6.1-жадвал).

6.1-жадвал

Кирилл алифбоси ўзбек ҳарфлари

t=	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
k=0	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О
	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
k=3	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С

16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ъ	Э	Ю	Я
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ъ	Э	Ю	Я	А	Б	В

6.1-вазифа. ФАКУЛЬТЕТ матнини Цезар усули билан шифирланг.

Бажариш усули.

Берилган. $T_{матн}$ = {ФАКУЛЬТЕТ}, $T_{шифрматн}$ = ?

Бу усулда 1 –жадвалнинг k = 0 сатридаги Ф ҳарфи топилади.

Бу ҳарфга k = 3 сатрдаги Ч ҳарфи мос келади. Демак,

Ф→Ч, А→Г, К→Н, У→Ц, Ь→Ю, Т→Х,Е→З, Т→Х алмаштиришлар олинади.

Жавоб. $T_{шифрланган\ матн}$ ={ЧГНЦЮХЗХ}

6.2-вазифа. ЭКОНОМИКА ФАКУЛЬТЕТИ матнини Цезар усули билан шифирланг.

Бажариш усули.

Берилган. $T_{матн}$ = {ЭКОНОМИКА ФАКУЛЬТЕТИ}, $T_{шифрматн}$ = ?

Бу усулда 6.1 –жадвалдан: Э→А, К→Н, О→С, Н→Р, … , И→Л алмаштиришлар олинади.

Жавоб. $T_{шифрланган\ матн}$={АНСРСПЛНГ ЧГНЦЮХЗХЛ}

6.3-вазифа. ИНСТИТУТ матнини Цезар усули билан шифирланг. Бажариш усули.

Берилган. $T_{матн}$ = {ИНСТИТУТ}, $T_{шифрматн}$ = ?

1 –жадвалдан: И→Л, Н→Р, С→ Ф, Т→Х, И→Л, Т→Х, У→Ц, Т→Х алмаштиришлар олинади.

Жавоб. $T_{шифрланган\ матн}$={ЛРФХЛХЦХ}.

6.4-вазифа. ЛРФХЛХЦХ матни Цезар усули билан шифирланган. Бу матнни дешифрланг.

Бажариш усули.

Берилган. $T_{шифрланган\ матн}$={ЛРФХЛХЦХ}, $T_{дешифрланган\ матн}$ = ?

Бу усулда 1 –жадвалнинг k = 3 сатридаги Л ҳарфи топилади.

Бу ҳарфга k = 0 сатрдаги И ҳарфи мос келади.

1 –жадвалдан: Л→И, Р→Н, Ф→С, Х→Т, Л→И, Х→Т, Ц→У, Х→Т алмаштиришлар олинади.

Жавоб. $T_{дешифрланган\ матн}$ = {ИНСТИТУТ}

6.2. Ахборотларни аффин тизимидаги Цезар усули билан шифрлаш

Афин тизимидаги Цезар усулида ҳар бир ҳарфга алмаштирувчи ҳарфлар махсус формула ёрдамида аниқланади:

$at + b(\mathrm{mod}\ m)$

Бу ерда a ва b – бутун сонлар, $a \geq 0$ ва $b \leq m$, ЭКУБ $(a, m)=1$

Математикадан маълумки $at + b(\mathrm{mod} m)$ ифода таққосламани ифодалайди. Чунки, a ва b бутун сонларни m бутун натурал сонга бўлинганда бир хил r ($0 \leq r < m$) қолдиқ ҳосил бўлса, a ва b сонлар m модул бўйича таққосланадиган (тенг қолдиқли) сонлар дейилади ва $a \equiv b(\mathrm{mod}\ m)$ кўринишда белгиланади.

Энди r ($0 \leq r < m$) қолдиқ ҳосил бўлса, a ва b сонлар m модул бўйича таққосланадиган (тенг қолдиқли) сонларга мисолллар келтирамиз.

1) 5 ни 32 га бўлганда 5 қолдиқ қолади. 5/32=0*32+5 ва қуйидаги муносабат ўринли бўлади: 5(mod32) ≡ 5.
2) 33 ни 32 га бўлганда 1 қолдиқ қолади. 33/32=1*32+1 ва қуйидаги муносабат ўринли бўлади: 33(mod32) ≡ 1.
3) 32 ни 32 га бўлганда 0 қолдиқ қолади. 32/32=1*32+0 ва қуйидаги муносабат ўринли бўлади: 32(mod32) ≡ 0
4) 83 ни 32 га бўлганда 19 қолдиқ қолади. 83/32=2*32+19 ва қуйидаги муносабат ўринли бўлади: 83(mod32) ≡ 19.
5) 92 ни 32 га бўлганда 28 қолдиқ қолади. 92/32=2*32+28 ва қуйидаги муносабат ўринли бўлади: 92(mod32) ≡ 28.

6. 5-вазифа.

1) Цезар жадвалини **3t+5** силжитишдаги кўриниши тузинг

2) $T_{матн}$ ={ ФАКУЛЬТЕТ } матнини Цезар жадвалини **3t+5** силжитишдаги кўриниши билан шифирланг.

Бажариш усули. Берилган. $T_{матн}$ = {ФАКУЛ ЬТЕТ}, $T_{шифрматн}$ = ?

1-қадам.

1) Цезар жадвалини **3t+5** силжитишдаги кўриниши тузамиз. Афин тизимидаги Цезар усулида ҳар бир ҳарфга алмаштирувчи ҳарфлар ушбу формула ёрдамида аниқлаймиз: $at + b(\mathrm{mod}\ \mathbf{m})$.

Алифбодаги ҳарфлар сони $m = 32$ (6.1-жадвал). $at + b = 3t+5$ дан $a = 3$ ва $b = 5$ га тенг.

Энди $at + b(\mathrm{mod}\ \mathbf{m}) = 3t+5(\mathrm{mod}32)$ учун ҳисоблашларни бажарамиз ва 6.2-жадвалга эга бўламиз:

1) t =0 да 3t+5(mod32) = 3*0+5(mod32) = 5(mod32) = 5;
2) t =1 да 3t+5(mod32) = 3*1+5(mod32) = 8(mod32) = 8;
3) t =2 да 3t+5(mod32) = 3*2+5(mod32) = 11(mod32) = 11;
4) t =3 да 3t+5(mod32) = 3*3+5(mod32) = 14(mod32) = 14;
5) t =4 да 3t+5(mod32) = 3*4+5(mod32) = 17(mod32) = 17;
6) t =5 да 3t+5(mod32) = 3*5+5(mod32) = 20(mod32) = 20;
7) t =6 да 3t+5(mod32) = 3*6+5(mod32) = 23(mod32) = 23;
8) t =7 да 3t+5(mod32) = 3*7+5(mod32) = 26(mod32) = 26;
9) t =8 да 3t+5(mod32) = 3*8+5(mod32) = 29(mod32) = 29;
10) t =9 да 3t+5(mod32) = 3*9+5(mod32) = 32(mod32) = 0;
11) t =10 да 3t+5(mod32) = 3*10+5(mod32) =35(mod32) = 3;
12) t =11 да 3t+5(mod32) = 3*11+5(mod32) = 38(mod32) = 6;
13) t =12 да 3t+5(mod32) = 3*12+5(mod32) = 41(mod32) = 9;
14) t =13 да 3t+5(mod32) = 3*13+5(mod32) = 44(mod32) = 12;
15) t =14 да 3t+5(mod32) = 3*14+5(mod32) = 47(mod32) = 15;
16) t =15 да 3t+5(mod32) = 3*15+5(mod32) = 50(mod32) = 18;
17) t =16 да 3t+5(mod32) = 3*16+5(mod32) =53(mod32) = 21;
18) t =17 да 3t+5(mod32) = 3*17+5(mod32) = 56(mod32) = 23;
19) t =18 да 3t+5(mod32) = 3*18+5(mod32) = 59(mod32) = 27;
20) t =19 да 3t+5(mod32) = 3*19+5(mod32) = 62(mod32) = 30;
21) t =20 да 3t+5(mod32) = 3*20+5(mod32) = 65(mod32) = 1;
22) t =21 да 3t+5(mod32) = 3*21+5(mod32) = 68(mod32) = 4;
23) t =22 да 3t+5(mod32) = 3*22+5(mod32) = 71 (mod32) = 7;
24) t =23 да 3t+5(mod32) = 3*23+5(mod32) = 74(mod32) = 10;
25) t =24 да 3t+5(mod32) = 3*24+5(mod32) = 77(mod32) = 13;
26) t =25 да 3t+5(mod32) = 3*25+5(mod32) = 80 (mod32) = 16;
27) t =26 да 3t+5(mod32) = 3*26+5(mod32) = 83(mod32) = 19;
28) t =27 да 3t+5(mod32) = 3*27+5(mod32) = 86(mod32) = 22;
29) t =28 да 3t+5(mod32) = 3*28+5(mod32) = 89(mod32) = 25;
30) t =29 да 3t+5(mod32) = 3*29+5(mod32) = 92(mod32) = 28;
31) t =30 да 3t+5(mod32) = 3*30+5(mod32) = 95(mod32) = 31;
32) t =31 да 3t+5(mod32) = 3*31+5(mod32) = 98 (mod32) = 2;

6.2-жадвал

t =	0	1	2	3	4	5
3t+5(mod32)	5	8	11	14	17	20

6	7	8	9	10	11	12
23	26	29	0	3	6	9

13	14	15	16	17	18	19
12	15	18	21	23	27	30

20	21	22	23	24	25	26
1	4	7	10	13	16	19

27	28	29	30	31		
22	25	28	31	2		

2-қадам.

Навбатдаги Цезар жадвалини тузиш учун t= сатрдаги 0, 1, 2,… ва 3t+5 сатрдаги 5,8,11,… кодларга мос ҳарфларни қўйиб чиқамиз.

6.3-жадвал.

Цезар жадвалини 3t+5 силжитишдаги кўриниши.

t =	А	Б	В	Г	Д	Е
3t+5(mod32)	Е	З	К	Н	Р	У

Ё	Ж	З	И	Й	К	Л
Ц	Щ	Э	А	Г	Ё	И

М	Н	О	П	Р	С	Т
Л	О	С	Ф	Ц	Ь	Ю

У	Ф	Х	Ц	Ч	Ш	Щ
Б	Д	Ж	Й	М	П	Т

Ь	Ъ	Э	Ю	Я		
Х	Ш	Ъ	Я	В		

3-қадам.

2) Энди $Т_{матн}$ ={ФАКУЛЬТЕТ} матнини Цезар жадвалини **3t+5** силжитиш бўйича ҳосил қилинган 6.3-жадвал асосида шифрлашга ўтамиз

Берилган. $Т_{матн}$ = {ФАКУЛ ЬТЕТ}, $Т_{шифрматн}$ = ?

Бу усулда 6.3 –жадвалнинг k = 0 сатридаги Ф ҳарфи топилади.

Бу ҳарфга **3t+5** сатрдаги Д ҳарфи мос келади. Демак,

Ф→Д, А→Е, К→Ё, У→Б, Л→И, Ь→Ц, Т→Ю, Е→У, Т→Ю алмаштиришлар олинади.

Жавоб. $T_{шифрланган\ матн}$ ={ДЕЁБИЦЮУЮ}

6.6-вазифа. ЭКОНОМИКА ФАКУЛЬТЕТИ матнини Цезар жадвалини 3t+5 силжитишдаги усули билан шифирланг.

Бажариш усули.

Берилган. $T_{матн}$ = {ЭКОНОМИКА ФАКУЛЬТЕТИ}, $T_{шифрматн}$ = ?

Бу усулда 6.3 –жадвалдан: Э→Ъ, К→Ё, О→С, Н→О, … , И→А алмаштиришлар олинади.

Жавоб. $T_{шифрланган\ матн}$ ={ЪЁСОСПАЁЕ ДЕЁБИЦЮУЮА}

6.7-вазифа. ИНСТИТУТ матнини Цезар жадвалини 3t+5 силжитишдаги кўриниши билан шифрланг.

Бажариш усули.

Берилган. $T_{матн}$ = {ИНСТИТУТ}, $T_{шифрматн}$ = ?

6.3 –жадвалидан: И→А, Н→О, С→ Ь, Т→Ю, И→А, Т→Ю, У→Е, Т→Ю алмаштиришлар олинади.

Жавоб. $T_{шифрланган\ матн}$ ={АОЬЮАЮЕЮ}.

6.8-вазифа. ДЕЁБИЦЮУЮ матни Цезар жадвалини 3t+5 силжитишдаги кўриниши билан шифирланган. Бу матнни дешифрланг.

Бажариш усули.

Берилган. $T_{шифрланган\ матн}$ ={ДЕЁБИЦЮУЮ}, $T_{дешифрланган\ матн}$ = ?

Бу усулда 6.3 –жадвалнинг 3t+5 сатридаги Д ҳарфи топилади.

Бу ҳарфга t = 0 сатрдаги Ф ҳарфи мос келади.

2 –жадвалидан: Д→Ф, Е→А, Ё→К, Б→У, И→Л, Ц→Ь, Ю→Т, У→Е, Ю→Т алмаштиришлар олинади.

Жавоб. $T_{дешифрланган\ матн}$ = {ФАКУЛЬТЕТ}

6.3. Таянч сўзли Цезар усули

Мавзу мустақил ўрганилади.

Адабиёт: Алимов Р.Х, Ходиев Б.Ю., Алимов Қ.А., Усмонов С.У., Бегалов Б.Б., Зайналов Н.Р., Мусалиев А.А., Файзиева Ф. Миллий иқтисодда ахборот тизимлари ва технологиялари. «Шарқ» нашриёт-матбаа акциядорлик компанияси бош таҳририяти. Тошкент -2004 Мавзу 259-261 бетлардан ёритилган.

$=\{21\ 01\ 11\ 20\ 12\ 29\ 19\ 18\ 19\}$.

- Энди r_i - гамма матнни $r_1\ r_2\ r_3\ r_4\ r_5\ r_6\ r_7\ r_8\ r_9$ харфларининг кодлари аниқлаймиз:
- $T_{\text{гамма матн}} = \{\text{САРДОРБЕК}\} = \{r_1\ r_2\ r_3\ r_4\ r_5\ r_6\ r_7\ r_8\ r_9\} =$
  $= \{18\ 01\ 17\ 05\ 15\ 17\ 02\ 06\ 11\}$.
- $T_{\text{шифрланган матн}} = \{c_1\ c_2\ c_3\ c_4\ c_5\ c_6\ c_7\ c_8\ c_9\} = ?$

Энди (1) формулага кўра қуйидаги ҳисоблашлашларни бажрамиз:

1) $c_1 = (m_1+r_1)\text{mod}(33) = (21+18)\text{mod}(33) = 39\text{mod}(33) = 6.$ ☛
   39 сонини 33 га бўлганда 6 қолдиқ қолади, $39=33*1+6$;
2) $c_2 = (m_2+r_2)\text{mod}\ 33 = (1+1)\text{mod}(33) = 2\ \text{mod}(33) = 2.$ ☛
   2 сонини 33 га бўлганда 2 қолдиқ қолади, $2=33*0+2$;
3) $c_3 = (m_3+r_3)\text{mod}(33) = (11+17)\text{mod}(33) = 28\text{mod}(33) = 28.$ ☛
   28 сонини 33 га бўлганда 28 қолдиқ қолади, $28=33*0+28$:
4) $c_4 = (m_4+r_4)\text{mod}(33) = (20+5)\text{mod}(33) = 25\text{mod}(33) = 25;$ ☛
5) $c_5 = (m_5+r_5)\text{mod}(33) = (12+15)\text{mod}(33) = 27\text{mod}(33) = 27;$ ☛
6) $c_6 = (m_6+r_6)\text{mod}(33) = (29+17)\text{mod}(33) = 46\ \text{mod}(33) = 13;$ ☛
   46 сонини 33 га бўлганда 13 қолдиқ қолади, $46=33*1+13$;
7) $c_7 = (m_7+r_7)\text{mod}(33) = (19+2)\text{mod}(33) = 21\text{mod}(33) = 21;$ ☛
8) $c_8 = (m_8+r_8)\text{mod}(33) = (18+6)\text{mod}(33) = 24\ \text{mod}(33) = 24;$ ☛
9) $c_9 = (m_9+r_9)\text{mod}(33) = (19+11)\text{mod}(33) = 30\text{mod}(33) = 30;$ ☛

$T_{\text{шифрланган матн}} = \{c_1\ c_2\ c_3\ c_4\ c_5\ c_6\ c_7\ c_8\ c_9\} =$
$\{06\ \ 02\ 28\ \ 25\ 27\ 13\ \ 21\ 24\ 30\}$

Топилган кодларга кўра 7.1 жадвалдан мос ҳарфларни қуйиб чиқамиз.

Жавоб.

$T_{\text{шифрланган матн}} = \{\text{ЕБЫШЪМФЧЭ}\}$.

7.2-вазифа.

САРДОРБЕК гамма матн билан шифрланган ЕБЫШЪМФЧЭ матни дешифрланг.

Вазифанинг бажарилиши.

- Берилган: $T_{\text{шифрланган матн}} = \{\text{ЕБЫШЪМФЧЭ}\}$,
  $T_{\text{гамма матн}} = \text{САРДОРБЕК}\}$.
- Очиқ ва гамма матндаги ҳарфлар сони тенг ва 9 та, $i = 9$.
- Жадвалдаги жами ҳарфлар сони 33 та. $N = 33$.
- Қоидага кўра, c_i – шифрланган матнни 9 та $c_1\ c_2\ c_3\ c_4\ c_5\ c_6\ c_7\ c_8\ c_9$ харфларининг кодлари 7.1-жадвалга асосан қуйидагича бўлади:
- $T_{\text{шифрланган матн}} = \{\text{ЕБЫШЪМФЧЭ}\} = \{c_1\ c_2\ c_3\ c_4\ c_5\ c_6\ c_7\ c_8\ c_9\} =$
  $= \{06\ \ 02\ 28\ \ 25\ 27\ 13\ \ 21\ 24\ 30\}$
- Энди r_i - гамма матнни $r_1\ r_2\ r_3\ r_4\ r_5\ r_6\ r_7\ r_8\ r_9$ харфларининг кодлари аниқлаймиз:
- $T_{\text{гамма матн}} = \{\text{САРДОРБЕК}\} = \{r_1\ r_2\ r_3\ r_4\ r_5\ r_6\ r_7\ r_8\ r_9\}$
  $= \{18\ 01\ 17\ \ 05\ 15\ \ 17\ 02\ \ 06\ \ 11\}$.
- $T_{\text{матн}} = \{\text{ФАКУЛЬТЕТ}\} = \{m_1\ m_2\ m_3\ m_4\ m_5\ m_6\ m_7\ m_8\ m_9\} = ?$

Энди (2) формулага кўра қуйидаги ҳисоблашлашларни бажрамиз:

1) $m_1 = (c_1 - r_1) \bmod(33) = (6-18) \bmod(33) = -12 \bmod(33) =$
$(-33+21) \bmod(33) = 21 \bmod(33) = 21;$

Изоҳ.

- Таққосламада манфий ишорали сон ишлатилмайди. Бундай ҳолларда mod(33) модулни манфий ишорали (-33) сонига шундай x сонини қўшамизки натижа - 12 бўлсин. Яъни, $-33 + x = -12$.
Бундан $x = 33 - 12 = 21$.
- Демак, $-12 \bmod 33 = (-33+21) \bmod(33) = 21 \bmod 33 = 21;$
- Юқорида келтирилган теоремалардан чиқадиган хулосаларга кўра таққосламаларда манфий сон инобатга олинмайди ва ташлаб юборилади: $(-33+21) \bmod(33) = 21 \bmod(33)$

2) $m_2 = (c_2 - r_2) \bmod(33) = (2-1) \bmod(33) = 1 \bmod(33) = 1;$
3) $m_3 = (c_3 - r_3) \bmod(33) = (28-17) \bmod(33) = 11 \bmod(33) = 11;$
4) $m_4 = (c_4 - r_4) \bmod(33) = (25-5) \bmod(33) = 20 \bmod(33) = 20;$
5) $m_5 = (c_5 - r_5) \bmod(33) = (27-15) \bmod(33) = 12 \bmod(33) = 12;$
6) $m_6 = (c_6 - r_6) \bmod(33) = (13-17) \bmod(33) = -4 \bmod(33) =$
$= (-33+29) \bmod(33) = 29 \bmod(33) = 29$ (изоҳга қаранг);
7) $m_7 = (c_7 - r_7) \bmod(33) = (21-2) \bmod(33) = 19 \bmod(33) = 19;$
8) $m_8 = (c_8 - r_8) \bmod(33) = (24-6) \bmod(33) = 18 \bmod(33) = 18;$
9) $m_9 = (c_9 - r_9) \bmod(33) = (30-11) \bmod(33) = 19 \bmod(33) = 19.$

Биз 1- жадвалдаги m_i – шифрланган матнни $m_1\, m_2\, m_3\, m_4\, m_5\, m_6\, m_7 m_8 m_9$ ҳарфларининг кодлари аниқладик:

$\{m_1\ m_2\ m_3\ m_4\ m_5\ m_6\ m_7\ m_8\ m_9\} = \{21\ 01\ 11\ 20\ 12\ 29\ 19\ 18\ 19\}$

Топилган кодларга кўра 7.1 жадвалдан мос ҳарфларни қуйиб чиксак олинган натижа дешифрланган матнни ифодалайди.

Жавоб.

$T_{\text{шифрланган матн}} = \{21\ 01\ 11\ 20\ 12\ 29\ 19\ 18\ 19\} = \{\text{ФАКУЛЬТЕТ}\}.$

Амалий машғулот вазифалари

I.Дарснинг мақсади. Талабаларни ахборот ҳимояси, ахборот хавфсизлигида ишлатиладиган таққосламалар ҳақида асосий тушунчаларни бериш ва ахборотларни гаммалаш усули билан шифрлаш ва дешифрлашни ўргатиш.

II. Информацион техник ва услубий воситалар

II.1. Pentium компьютерлари, кадоскоп, видеоплеер ва плакатлар

II.2. Адабиётлар: [1, 2, 3, 4, 5, 6, 7] ва мавзу бўйича тарқатма материалллар

7.1.1-вазифа.

1)ЛАБОРАТОРИЯ очиқ матли хабарини, МАШГУЛОТЛАР гамма матн билан шифрланг;

2) Гаммалаш усули билан бажариладиган амалларни таснифланг.

3) Шифрланган матнни дешифрланг.

7.1.2-вазифа.

1)МАТЕМАТИК очиқ матли хабарини, МОДЕЛЛАРИ гамма матн билан шифрланг;

2) Гаммалаш усули билан бажариладиган амалларни таснифланг.

3) Шифрланган матнни дешифрланг.

7.1.3-вазифа.

1) МАШГУЛОТЛАР очиқ матли хабарини, ЛАБОРАТОРИЯ гамма матн билан шифрланг;

2) Гаммалаш усули билан бажариладиган амалларни таснифланг.

3) Шифрланган матнни дешифрланг.

7.1.4-вазифа.

1) МОДЕЛЛАРИ очиқ матли хабарини МАТЕМАТИК гамма матн билан шифрланг;

2) Гаммалаш усули билан бажариладиган амалларни таснифланг.

3) Шифрланган матнни дешифрланг.

7.1.5-вазифа.

1) КОМПЬЮТЕР очиқ матли хабарини МАТЕМАТИК гамма матн билан шифрланг;

2) Гаммалаш усули билан бажариладиган амалларни таснифланг.

3) Шифрланган матнни дешифрланг.

7.1.6-вазифа.

1) МАТЕМАТИК очиқ матли хабарини КОМПЬЮТЕР гамма матн билан шифрланг;

2) Гаммалаш усули билан бажариладиган амалларни таснифланг.

3) Шифрланган матнни дешифрланг.

7.1.7-вазифа.

1) МАТЕМАТИКА очиқ матли хабарини ХУЖАММУРОД гамма матн билан шифрланг;

2) Гаммалаш усули билан бажариладиган амалларни таснифланг.

3) Шифрланган матнни дешифрланг.

7.1.8-вазифа.

1) ЛАБОРАТОРИЯ очиқ матли хабарини ХУЖАМУРОДОВ гамма матн билан шифрланг;

2) Гаммалаш усули билан бажариладиган амалларни таснифланг.

3) Шифрланган матнни дешифрланг.

7.1.9-вазифа.

1) СЕРТИФИКАТ очиқ матли хабарини МАТЕМАТИКА гамма матн билан шифрланг;

2) Гаммалаш усули билан бажариладиган амалларни таснифланг.

3) Шифрланган матнни дешифрланг.

7.1.10-вазифа.

1) АХБОРОТЛАР очиқ матли хабарини ТЕХНОЛОГИЯ гамма матн билан шифрланг;

2) Гаммалаш усули билан бажариладиган амалларни таснифланг.

3) Шифрланган матнни дешифрланг.

7.1.11-вазифа.

1) ТЕХНОЛОГИЯ очиқ матли хабарини АХБОРОТЛАР гамма матн билан шифрланг;

2) Гаммалаш усули билан бажариладиган амалларни таснифланг.

3) Шифрланган матнни дешифрланг.

7.1.12-вазифа.

1) САМАНДАРБЕК очиқ матли хабарини АХБОРОТЛАРИ гамма матн билан шифрланг;

2) Гаммалаш усули билан бажариладиган амалларни таснифланг.

3) Шифрланган матнни дешифрланг.

Лаборатория иши вазифалари

I.Дарснинг мақсади. Талабаларни ахборот ҳимояси, ахборот хавфсизлигида ишлатиладиган таққосламалар ҳақида асосий тушунчаларни бериш ва ахборотларни гаммалаш усули билан шифрлаш ва дешифрлашни ўргатиш.

II. Информацион техник ва услубий воситалар

II.1. Pentium компьютерлари, кадоскоп, видеоплеер ва плакатлар

II.2. Адабиётлар: [1, 2, 3, 4, 5, 6, 7] ва мавзу бўйича тарқатма материаллар

7.2.01- 7.2.26 - Вариантлар топшириқлари

1) {...} очиқ матли хабарини {...} гамма матн билан шифрланг

2) Шифрланган матнни дешифрланг.

3) Гаммалаш усули билан бажариладиган амалларни таснифланг.

Изоҳ. Очиқ матнда талабанинг исми шарифи олинади, гамма матнни талабанинг ўзи танлайди.

Кўрсатма.

Ҳар бир талаба берилган топшириқ бўйича гуруҳ журналдаги фамилияси исми шарифи бўйича вариант вазифасини тузади.

Масалан, «Иқтисодиёт ва бошқарув» факультети 202- гуруҳ талабаси Аликулова Азиза гуруҳ журналидаги тартиб рақами 10 бўлсин.

Бу талаба учун вазифа варианти қуйидагича тузилади.

7.2.10 - Вариант.

а) топшириқ

1) {РАХИМОВ} очиқ матли хабарини {АХБОРОТ} гамма матн билан шифрланг

2) Шифрланган матнни дешифрланг.

3) Гаммалаш усули билан бажариладиган амалларни таснифланг.

б) топшириқ

1) {САРДОР} очиқ матли хабарини {ТАЛАБА} гамма матн билан шифрланг

2) Шифрланган матнни дешифрланг.

3) Гаммалаш усули билан бажариладиган амалларни таснифланг.

8.Мавзу. Ахборотларни симметрик усул билан шифрлаш. Вижинер усули

8.1.Ахборотларни Вижинер жадвали билан оддий шифрлаш усули
8.2. Ахборотларни Вижинер жадвали билан калитли шифрлаш

I.Дарснинг мақсади. Талабаларга ахборот хавфсизлиги, ахборот ҳимоясида Вижинер жадвали билан ахборотларни оддий, калитли шифрлаш ва дешифрлаш усулларини ўргатиш.
II. Информацион техник ва услубий воситалар
II.1. Pentium компьютерлари, кадоскоп, видеоплеер ва плакатлар
II.2. Адабиётлар: [1, 2, 3, 4, 5, 6, 7] ва мавзу бўйича тарқатма материалллар

Криптографияда алмаштиришнинг ярималфавитли усул деб номланувчи Вижинер усули ҳисобланади. У квадрат матрица кўринишида бўлиб, рус алифбоси ҳарфларидан иборат бўлади. Биринчи сатрда ҳарфлар алифбо тартибида жойлашади. Иккинчи сатрни биринчи позициясига алифбо ҳарфларнинг иккинчи ҳарфларидан бошлаб тартиб билан ёзилади, Биринчи А ҳарфи эса охирги позицияга ёзилади ва ҳ.к.

8.1-жадвал. Вижинер жадвали

А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ъ	Ы	Э	Ю	Я	_
Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ъ	Ы	Э	Ю	Я	_	А
В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ъ	Ы	Э	Ю	Я	_	А	Б
Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ъ	Ы	Э	Ю	Я	_	А	Б	В
Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ъ	Ы	Э	Ю	Я	_	А	Б	В	Г
Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ъ	Ы	Э	Ю	Я	_	А	Б	В	Г	Д
Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ъ	Ы	Э	Ю	Я	_	А	Б	В	Г	Д	Е
З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ъ	Ы	Э	Ю	Я	_	А	Б	В	Г	Д	Е	Ж
И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ъ	Ы	Э	Ю	Я	_	А	Б	В	Г	Д	Е	Ж	З
Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ъ	Ы	Э	Ю	Я	_	А	Б	В	Г	Д	Е	Ж	З	И
К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ъ	Ы	Э	Ю	Я	_	А	Б	В	Г	Д	Е	Ж	З	И	Й
Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ъ	Ы	Э	Ю	Я	_	А	Б	В	Г	Д	Е	Ж	З	И	Й	К
М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ъ	Ы	Э	Ю	Я	_	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л
Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ъ	Ы	Э	Ю	Я	_	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М
О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ъ	Ы	Э	Ю	Я	_	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н
П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ъ	Ы	Э	Ю	Я	_	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О
Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ъ	Ы	Э	Ю	Я	_	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П
С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ъ	Ы	Э	Ю	Я	_	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р
Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ъ	Ы	Э	Ю	Я	_	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С
У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ъ	Ы	Э	Ю	Я	_	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т
Ф	Х	Ц	Ч	Ш	Щ	Ь	Ъ	Ы	Э	Ю	Я	_	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У
Х	Ц	Ч	Ш	Щ	Ь	Ъ	Ы	Э	Ю	Я	_	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф
Ц	Ч	Ш	Щ	Ь	Ъ	Ы	Э	Ю	Я	_	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х
Ч	Ш	Щ	Ь	Ъ	Ы	Э	Ю	Я	_	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц
Ш	Щ	Ь	Ъ	Ы	Э	Ю	Я	_	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч
Щ	Ь	Ъ	Ы	Э	Ю	Я	_	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш
Ь	Ъ	Ы	Э	Ю	Я	_	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ
Ъ	Ы	Э	Ю	Я	_	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь
Ы	Э	Ю	Я	_	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ъ
Э	Ю	Я	_	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ъ	Ы
Ю	Я	_	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ъ	Ы	Э
Я	_	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ъ	Ы	Э	Ю
_	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ъ	Ы	Э	Ю	Я

8.1.Ахборотларни Вижинер жадвали билан оддий шифрлаш

8.1-вазифа. ЛАБОРОТОРИЯ ИШИ матнини Вижинер жадвалидан фойдаланиб шифрланг.

Вазифанинг бажарилиши.

$Т_{матн}$ = {ЛАБОРОТОРИЯ _ИШИ}, $Т_{шифрланган\ матн}$ = ?

Тушунарли бўлиш учун калит ва шифрланадиган матн ҳарфларидан жадвал тузамиз.

Матн	Л	А	Б	О	Р	О	Т	О	Р	И	Я	_	И	Ш	И
Шифрланган матн	Ц	А	В	Ы	_	Ы	Д	Ы	_	Р	Э	Я	Р	П	Р

1) Л ҳарфига мос келадиган шифрланган ҳарф қуйидагича топилади:

1-қадам: Биринчи устундан Л ҳарфли сатрни танлаймиз;

2-қадам: Биринчи сатрдан Л ҳарфли устунни танламиз;

3-қадам: Л ҳарфли сатр ва Л ҳарфли устуннинг кесишишидаги ҳарф танланади, яъни $Л^{сатр} \rightarrow Л^{устун} \rightarrow Ц$;

2) А ҳарфига мос келадиган шифрланган ҳарф қуйидагича топилади:

1-қадам: Биринчи устундан А ҳарфли сатрни танлаймиз;

2-қадам: Биринчи сатрдан А ҳарфли устунни танламиз;

3-қадам: А ҳарфли сатр ва А ҳарфли устуннинг кесишишидаги ҳарф танланади, яъни $А^{сатр} \rightarrow А^{устун} \rightarrow А$;

3) Бу алмаштиришларни матннинг бошқа ҳарфлари учун ҳам амалга оширамиз:

$Б^{сатр} \rightarrow Б^{устун} \rightarrow В$; $О^{сатр} \rightarrow О^{устун} \rightarrow Ы$; $Р^{сатр} \rightarrow Р^{устун} \rightarrow \_$; $О^{сатр} \rightarrow О^{устун} \rightarrow Ы$;
$Р^{сатр} \rightarrow Р^{устун} \rightarrow \_$; $И^{сатр} \rightarrow И^{устун} \rightarrow Р$; $Я^{сатр} \rightarrow Я^{устун} \rightarrow Э$; $\_^{сатр} \rightarrow \_^{устун} \rightarrow Я$;
$И^{сатр} \rightarrow И^{устун} \rightarrow Р$; $Ш^{сатр} \rightarrow Ш^{устун} \rightarrow П$; $И^{сатр} \rightarrow И^{устун} \rightarrow Р$;

Жавоб: $Т_{шифрланган\ матн}$ = {ЦАВЫ_ЫДЫ_РЭЯРПР}

8.2-вазифа. $Т_{шифрланган\ матн}$ = {ИКФАЬАГ} билан қандай сўз шифрланган. Вижинер жадвали билан шифрланган матнни дешифланг.

Вазифанинг бажарилиши

1) Шифрланган матндаги И ҳарфига мос келадиган ҳарф қуйидагича топилади:

1-қадам: Биринчи устундан И ҳарфли сатрни танлаймиз;

2-қадам: Биринчи сатрдан И ҳарфли устунни танламиз;

3-қадам: И ҳарфли сатр ва И ҳарфли устуннинг кесишишидаги ҳарф танланади, яъни $И^{сатр} \rightarrow И^{устун} \rightarrow Д$;

2) Шифрланган матндаги К ҳарфига мос келадиган ҳарф қуйидагича топилади:

1-қадам: Биринчи устундан К ҳарфли сатрни танлаймиз;

2-қадам: Биринчи сатрдан К ҳарфли устунни танламиз;

3-қадам: К ҳарфли сатр ва К ҳарфли устуннинг кесишишидаги ҳарф танланади, яъни $К^{сатр} \rightarrow К^{устун} \rightarrow Е$;

3) Шифрланган матннинг қолган ҳарфлари учун ҳам тегишли алмаштиришларни бажарамиз: $Ф^{сатр} \rightarrow Ф^{устун} \rightarrow К$; $А^{сатр} \rightarrow А^{устун} \rightarrow А$;
$Ь^{сатр} \rightarrow Ь^{устун} \rightarrow Н$; $А^{сатр} \rightarrow А^{устун} \rightarrow А$; $Г^{сатр} \rightarrow Г^{устун} \rightarrow Т$.

Дешифрланган матн	И	К	Ф	А	Ь	А	Г
Шифрланган матн	Д	Е	К	А	Н	А	Т

Жавоб: $T_{\text{дешифрланган матн}}$ = {ДЕКАНАТ}

8.2. Ахборотларни Вижинер жадвали билан калитли шифрлаш

8.3-вазифа. ТЕХНОЛОГИЯЛАР сўзини ИЛМ калит сўз орқали Вижинер жадвалидан фойдаланиб шифрланг.

Вазифанинг бажарилиши.

$T_{\text{калит}}$={ИЛМ}, $T_{\text{матн}}$ = {ТЕХНОЛОГИЯЛАР}, $T_{\text{шифрланган матн}}$ = ?

Тушунарли бўлиш учун калит ва шифрланадиган матн ҳарфларидан жадвал тузамиз. Шифрланадиган матндаги ҳарфлар сони 13 та. Жадвалда ИЛМ калит сўзи матндаги ҳарфлар сонига қараб тўлдирилади.

Матн	Т	Е	Х	Н	О	Л	О	Г	И	Я	Л	А	Р
Калит сўз	И	Л	М	И	Л	М	И	Л	М	И	Л	М	И
Шифрланган матн	Ь	Р	А	Х	Щ	Ч	Ц	О	Ф	Ж	Ц	М	Ш

Вижинер жадвали ёрдамида берилган матн қуйидагича шифрланади:

1) Калит сўзидаги “И” ҳарфли сатрни Вижинер жадвалдаги 1- устундан, матндаги “Т” ҳарфли устунни эса 1-сатрдан танлаймиз. “И” ҳарфли сатр ва “Т” ҳарфли устунлар кесишмасидаги “Ь” ҳарфи олинади. ($И^{\text{сатрдан}} \rightarrow Т^{\text{устундан}} \rightarrow Ь$)

2) Калит сўзидаги “Л” ҳарфини Вижинер жадвалдаги 1- устундан, матндаги “**Е**” ҳарфини эса 1-сатрдан танлаймиз. “**Л**” ҳарфли сатр ва “**Е**” ҳарфли устунлар кесишмасидаги “**Р**” ҳарфи олинади. ($Л^{\text{сатрдан}} \rightarrow Е^{\text{устундан}} \rightarrow \mathbf{Р}$)

3) Бу жараённи қолган ҳарфлар учун ҳам амалга оширамиз:

$М^{\text{сатрдан}} \rightarrow Х^{\text{устундан}} \rightarrow А$, $И^{\text{сатрдан}} \rightarrow Н^{\text{устундан}} \rightarrow Х$, $Л^{\text{сатрдан}} \rightarrow О^{\text{устундан}} \rightarrow Щ$,

$М^{\text{сатрдан}} \rightarrow И^{\text{устундан}} \rightarrow Ч$, $И^{\text{сатрдан}} \rightarrow О^{\text{устундан}} \rightarrow Ц$, $Л^{\text{сатрдан}} \rightarrow Г^{\text{устундан}} \rightarrow О$,

$М^{\text{сатрдан}} \rightarrow И^{\text{устундан}} \rightarrow Ф$, $И^{\text{сатрдан}} \rightarrow Я^{\text{устундан}} \rightarrow Ж$, $Л^{\text{сатрдан}} \rightarrow Л^{\text{устундан}} \rightarrow Ц$,

$М^{\text{сатрдан}} \rightarrow А^{\text{устундан}} \rightarrow М$, $И^{\text{сатрдан}} \rightarrow Р^{\text{устундан}} \rightarrow Ш$,

Жавоб: $T_{\text{калит}}$={ИЛМ}, $T_{\text{шифрланган матн}}$ = {ЬРА ХЩЧ ЦОФ ЖЦМ Ш}

8.4-вазифа.

$T_{\text{шифрланган матн}}$ = {РФФТЩБЬСХАУСЦА}

матни БИЛИМ калит сўз билан Вижинер жадвалидан фойдаланиб шифрланган. Бу матнни дешифрланг

Вазифанинг бажарилиши.

$T_{\text{калит}}$={БИЛИМ}, $T_{\text{шифрланган матн}}$ = {РФФТЩБЬСХАУСЦА}

$T_{\text{дешифрланган матн}}$ = ?

Калит ва шифрланадиган матн ҳарфларидан жадвал тузамиз. Шифрланган матндаги ҳарфлар сони 14 та. Бу жадвалда ҳам БИЛИМ калит сўзи шифрланган матндаги ҳарфлар сонига қараб тўлдирилади.

Калит сўз	Б	И	Л	И	М	Б	И	Л	И	М	Б	И	Л	И
Шифрланган матн	Р	Ф	Ф	Т	Щ	Б	Ь	С	Х	А	У	С	Ц	А
Дешифрланган матн	О	Л	И	Й	М	А	Т	Е	М	А	Т	И	К	А

Амалий машғулот вазифалари

I.Дарснинг мақсади. Талабаларга ахборот хавфсизлиги, ахборот ҳимоясида Вижинер жадвали билан ахборотларни оддий, калитли шифрлаш ва дешифрлаш усулларини ўргатиш.

II. Информацион техник ва услубий воситалар

II.1. Pentium компьютерлари, кадоскоп, видеоплеер ва плакатлар

II.2. Адабиётлар: [1, 2, 3, 4, 5, 6, 7] ва мавзу бўйича тарқатма материаллар

8.1.1-вазифа.

а) топшириқ

1)$Т_{матн}$ ={ОЛИЙ МАТЕМАТИКА ВА АХБОРОТ ТЕХНОЛОГИЯЛАРИ КАФЕДРАСИ} матнини Вижинер жадвалидан фойдаланиб шифрланг;

2) Шифрланган матнни дешифрланг;

3) Бажарилган ишларни изоҳланг. Алмаштиришларнинг схематик кўринишини келтиринг.

б) топшириқ

1)К={ТАЛАБА} калит сўзи билан $Т_{матн}$ ={ОЛИЙ МАТЕМАТИКА ВА АХБОРОТ ТЕХНОЛОГИЯЛАРИ КАФЕДРАСИ} матнини Вижинер жадвалидан фойдаланиб шифрланг;

2) К={ТАЛАБА} калит сўзи билан шифрланган матнни дешифрланг;

3) Бажарилган ишларни изоҳланг. Алмаштиришларнинг схематик кўринишини келтиринг.

8.1.2-вазифа.

а) топшириқ

1) $Т_{матн}$ ={ИНФОРМАТИКА ВА АХБОРОТ ТЕХНОЛОГИЯЛАРИ КАФЕДРАСИ} матнини Вижинер жадвалидан фойдаланиб шифрланг;

2) Шифрланган матнни дешифрланг;

3) Бажарилган ишларни изоҳланг. Алмаштиришларнинг схематик кўринишини келтиринг

б) топшириқ

1)К={МАГИСТР} калит сўзи билан $Т_{матн}$ ={ОЛИЙ МАТЕМАТИКА ВА АХБОРОТ ТЕХНОЛОГИЯЛАРИ КАФЕДРАСИ} матнини Вижинер жадвалидан фойдаланиб шифрланг;

2) К={МАГИСТР} калит сўзи билан шифрланган матнни дешифрланг;

3) Бажарилган ишларни изоҳланг. Алмаштиришларнинг схематик кўринишини келтиринг.

8.1.3-вариант.

а) топшириқ

1) $Т_{матн}$ ={МАТЕМАТИК БИЛИМЛАР БИЗГА ОМАД КЕЛТИРАДИ} матнини Вижинер жадвалидан фойдаланиб шифрланг;

2) Шифрланган матнни дешифрланг;

3) Бажарилган ишларни изоҳланг. Алмаштиришларнинг схематик кўринишини келтиринг

б) топшириқ

2) К={ОМАД} калит сўзи билан $Т_{матн}$ ={ОЛИЙ МАТЕМАТИКА ВА АХБОРОТ ТЕХНОЛОГИЯЛАРИ КАФЕДРАСИ} матнини Вижинер жадвалидан фойдаланиб шифрланг;

2) К={ОМАД} калит сўзи билан шифрланган матнни дешифрланг;

3) Бажарилган ишларни изоҳланг. Алмаштиришларнинг схематик кўринишини келтиринг

8.1.4-вазифа.

а) топшириқ

1) $Т_{матн}$ ={ИНФОРМАТИКА КИБЕРНЕТИКА ФАНЛАРИГА КИРАДИ} матнини Вижинер жадвалидан фойдаланиб шифрланг;

2) Шифрланган матнни дешифрланг;

3) Бажарилган ишларни изоҳланг. Алмаштиришларнинг схематик кўринишини келтиринг

б) топшириқ

2) К={ИНСТИТУТ} калит сўзи билан $Т_{матн}$ ={ОЛИЙ МАТЕМАТИКА ВА АХБОРОТ ТЕХНОЛОГИЯЛАРИ КАФЕДРАСИ} матнини Вижинер жадвалидан фойдаланиб шифрланг;

2) К={ИНСТИТУТ} калит сўзи билан шифрланган матнни дешифрланг;

3) Бажарилган ишларни изоҳланг. Алмаштиришларнинг схематик кўринишини келтиринг

8.1.5-вазифа.

а) топшириқ

1) $Т_{матн}$ ={ОЛИЙ МАТЕМАТИКА ВА ЭХТИМОЛЛАР НАЗАРИЯСИ} матнини Вижинер жадвалидан фойдаланиб шифрланг;

2) Шифрланган матнни дешифрланг;

3)Бажарилган ишларни изоҳланг. Алмаштиришларнинг схематик кўринишини келтиринг

б) топшириқ

1)К={ФАКУЛЬТЕТ} калит сўзи билан $Т_{матн}$ ={ОЛИЙ МАТЕМАТИКА ВА АХБОРОТ ТЕХНОЛОГИЯЛАРИ КАФЕДРАСИ} матнини Вижинер жадвалидан фойдаланиб шифрланг;

2) К={ФАКУЛЬТЕТ} калит сўзи билан шифрланган матнни дешифрланг;

3)Бажарилган ишларни изоҳланг. Алмаштиришларнинг схематик кўринишини келтиринг

8.1.6-вазифа.

а) топшириқ

1) $Т_{матн}$ ={ЭХТИМОЛЛАР НАЗАРИЯСИ ВА МАТЕМАТИК СТАТИСТИКА} матнини Вижинер жадвалидан фойдаланиб шифрланг;

2) Шифрланган матнни дешифрланг;

3) Бажарилган ишларни изоҳланг. Алмаштиришларнинг схематик кўринишини келтиринг

б) топшириқ

1) К={КАФЕДРА} калит сўзи билан $Т_{матн}$ ={ОЛИЙ МАТЕМАТИКА ВА АХБОРОТ ТЕХНОЛОГИЯЛАРИ КАФЕДРАСИ} матнини Вижинер жадвалидан фойдаланиб шифрланг;

2)К={КАФЕДРА} калит сўзи билан шифрланган матнни дешифрланг;
3) Бажарилган ишларни изоҳланг. Алмаштиришларнинг схематик кўринишини келтиринг

8.1.7-вазифа.

а) топшириқ

1) $T_{матн}$ ={ЙИГИРМА УЧИНЧИ ДЕКАБРЬ РЕСПУБЛИКА ПРЕЗИДЕНТИ САЙЛОВЛАРИ КУНИ} матнини Вижинер жадвалидан фойдаланиб шифрланг;
2) Шифрланган матнни дешифрланг;
3) Бажарилган ишларни изоҳланг. Алмаштиришларнинг схематик кўринишини келтиринг

б) топшириқ

1) К={ТАЛАБА} калит сўзи билан $T_{матн}$ ={ЙИГИРМА УЧИНЧИ ДЕКАБРЬ РЕСПУБЛИКА ПРЕЗИДЕНТИ САЙЛОВЛАРИ КУНИ} матнини Вижинер жадвалидан фойдаланиб шифрланг;
2)К={ТАЛАБА} калит сўзи билан шифрланган матнни дешифрланг;
3) Бажарилган ишларни изоҳланг. Алмаштиришларнинг схематик кўринишини келтиринг.

8.1.8-вазифа.

а) топшириқ

1) $T_{матн}$ ={МАМЛАКАТИМИЗ ДЕМОКРАТИК ДАВЛАТЛАР САФИДА БОРМОКДА} матнини Вижинер жадвалидан фойдаланиб шифрланг;
2)Шифрланган матнни дешифрланг;
3) Бажарилган ишларни изоҳланг. Алмаштиришларнинг схематик кўринишини келтиринг

б) топшириқ

1) К={САЙЛОВ} калит сўзи билан $T_{матн}$ ={ЙИГИРМА УЧИНЧИ ДЕКАБРЬ РЕСПУБЛИКА ПРЕЗИДЕНТИ САЙЛОВЛАРИ КУНИ} матнини Вижинер жадвалидан фойдаланиб шифрланг;
2)К={САЙЛОВ} калит сўзи билан шифрланган матнни дешифрланг;
3) Бажарилган ишларни изоҳланг. Алмаштиришларнинг схематик кўринишини келтиринг

8.1.9-вазифа.

а) топшириқ

1) $T_{матн}$ ={ДАСТУРИЙ ТАЪМИНОТ ДАСТУРЛАШ ТИЛЛАРИДА ЯРАТИЛАДИ} матнини Вижинер жадвалидан фойдаланиб шифрланг;
2) Шшифрланган матнни дешифрланг;
3) Бажарилган ишларни изоҳланг. Алмаштиришларнинг схематик кўринишини келтиринг

б) топшириқ

1) К={ДЕМОКРАТИЯ} калит сўзи билан $T_{матн}$ ={ЙИГИРМА УЧИНЧИ ДЕКАБРЬ РЕСПУБЛИКА ПРЕЗИДЕНТИ САЙЛОВЛАРИ КУНИ} матнини Вижинер жадвалидан фойдаланиб шифрланг;
2)К={ДЕМОКРАТИЯ} калит сўзи билан шифрланган матнни дешифрланг;
3) Бажарилган ишларни изоҳланг. Алмаштиришларнинг схематик кўринишини келтиринг

8.1.10-вазифа.

а) топшириқ

1) $Т_{матн}$ ={АХБОРОТ ТЕХНОЛОГИЯЛАРИ ФАН СИФАТИДА} матнини Вижинер жадвалидан фойдаланиб шифрланг;

2) Шифрланган матнни дешифрланг;

3) Бажарилган ишларни изоҳланг. Алмаштиришларнинг схематик кўринишини келтиринг

б) топшириқ

1) К={ПАРЛАМЕНТ} калит сўзи билан $Т_{матн}$ ={ЙИГИРМА УЧИНЧИ ДЕКАБРЬ РЕСПУБЛИКА ПРЕЗИДЕНТИ САЙЛОВЛАРИ КУНИ} матнини Вижинер жадвалидан фойдаланиб шифрланг;

2)К={ПАРЛАМЕНТ} калит сўзи билан шифрланган матнни дешифрланг;

3) Бажарилган ишларни изоҳланг. Алмаштиришларнинг схематик кўринишини келтиринг

8.1.11-вазифа.

а) топшириқ

1) $Т_{матн}$ ={ВИЖИНЕР ЖАДВАЛИ БИЛАН МАТННИ ШИФРЛАШ ВА ДЕШИФРЛАШ} матнини Вижинер жадвалидан фойдаланиб шифрланг;

2) Шифрланган матнни дешифрланг;

3) Бажарилган ишларни изоҳланг. Алмаштиришларнинг схематик кўринишини келтиринг

б) топшириқ

1) К={ИНСТИТУТ} калит сўзи билан $Т_{матн}$ ={ЙИГИРМА УЧИНЧИ ДЕКАБРЬ РЕСПУБЛИКА ПРЕЗИДЕНТИ САЙЛОВЛАРИ КУНИ} матнини Вижинер жадвалидан фойдаланиб шифрланг;

2)К={ИНСТИТУТ} калит сўзи билан шифрланган матнни дешифрланг;

3) Бажарилган ишларни изоҳланг. Алмаштиришларнинг схематик кўринишини келтиринг

8.1.12-вазифа.

а) топшириқ

1) $Т_{матн}$ ={АЛМАШТИРИШ УСУЛЛАРИДА ВИЖИНЕР ЖАДВАЛИДАН ФОЙДАЛАНИЛАДИ} матнини Вижинер жадвалидан фойдаланиб шифрланг;

2) Шифрланган матнни дешифрланг;

3) Бажарилган ишларни изоҳланг. Алмаштиришларнинг схематик кўринишини келтиринг

б) топшириқ

1) К={УМИД} калит сўзи билан $Т_{матн}$ ={ЙИГИРМА УЧИНЧИ ДЕКАБРЬ РЕСПУБЛИКА ПРЕЗИДЕНТИ САЙЛОВЛАРИ КУНИ} матнини Вижинер жадвалидан фойдаланиб шифрланг;

2)К={УМИД} калит сўзи билан шифрланган матнни дешифрланг;

3) Бажарилган ишларни изоҳланг. Алмаштиришларнинг схематик кўринишини келтиринг

Лаборатория иши вазифалари

I.**Дарснинг мақсади.** Лаборатория ишларини бажариш билан талабаларга ахборот хавфсизлиги, ахборот ҳимоясида Вижинер жадвали билан ахборотларни оддий, калитли шифрлаш ва дешифрлашни мустақил бажаришни ўргатиш.

II. Информацион техник ва услубий воситалар

II.1. Pentium компьютерлари, кадоскоп, видеоплеер ва плакатлар

II.2. Адабиётлар: [1, 2, 3, 4, 5, 6, 7] ва мавзу бўйича тарқатма материалллар

8.2.01 - 8.2.26 - Вариант.

- а) К={ТАЛАБА} ва б) К={МАГИСТР} калит сўзлари билан $T_{матн}$ ={ФАМИЛИЯ, ИСМ, ШАРИФ} матнини Вижинер жадвалидан фойдаланиб шифрланг;
- Берилган калит сўзи билан шифрланган матнни дешифрланг;
- Бажарилган ишларни изоҳланг. Алмаштиришларнинг схематик кўринишини келтиринг.

Кўрсатма.

Ҳар бир талаба берилган топшириқ бўйича гуруҳ журналдаги фамилияси исми шарифи бўйича вариант вазифасини тузади.

Масалан, «Иқтисодиёт ва бошқарув» факультети 202- гуруҳ талабаси Аликулова Азизанинг гуруҳ журналидаги тартиб рақами 10 бўлсин. Бу талаба учун вазифа варианти қуйидагича тузилади.

Мавзу. **Симметрик усул билан алмаштириш усуллари**. Вижинер жадвали билан ахборотларни шифрлаш

№ 8. Лаборатория иши вазифаси

8. 2. 10 - Вариант

а) топшириқ

1) К={ТАЛАБА} калит сўзи билан $T_{матн}$ ={АЛИКУЛОВА АЗИЗА} матнини Вижинер жадвалидан фойдаланиб шифрланг;

2) К={ТАЛАБА} калит сўзи билан шифрланган матнни дешифрланг;

3) Бажарилган ишларни изоҳланг. Алмаштиришларнинг схематик кўринишини келтиринг.

б) топшириқ

1) К={ МАГИСТР} калит сўзи билан $T_{матн}$ ={АЛИКУЛОВА АЗИЗА} матнини Вижинер жадвалидан фойдаланиб шифрланг;

2) К={МАГИСТР} калит сўзи билан шифрланган матнни дешифрланг;

3) Бажарилган ишларни изоҳланг. Алмаштиришларнинг схематик кўринишини келтиринг.

ёки талаба Сайдалиев Фаррух Фарходовичнинг гуруҳ журналидаги тартиб рақами 18 бўлса, унинг учун вазифа варианти қуйидагича тузилади:

8.2.18- Вариант

а) топшириқ

1) К={ТАЛАБА} калит сўзи билан $T_{матн}$ ={САЙДАЛИЕВ ФАРРУХ ФАРХОДОВИЧ} матнини Вижинер жадвалидан фойдаланиб шифрланг;

2) К={ТАЛАБА} калит сўзи билан шифрланган матнни дешифрланг;

3) Бажарилган ишларни изоҳланг. Алмаштиришларнинг схематик кўринишини келтиринг.

б) топшириқ

1) К={МАГИСТР} калит сўзи билан $T_{матн}$ ={САЙДАЛИЕВ ФАРРУХ ФАРХОДОВИЧ } матнини Вижинер жадвалидан фойдаланиб шифрланг;

2) К={МАГИСТР} калит сўзи билан шифрланган матнни дешифрланг;

3) Бажарилган ишларни изоҳланг. Алмаштиришларнинг схематик кўринишини келтиринг.

1-қадам. Берилган "САРДОР" сўзидаги ҳарфларини 9.1-жадвалга кўра кодларини аниқлаймиз:

$T_{матн}$ = {САРДОР} = $T_{код}$ = {18,1,17,5,15,17}.

Натижада, берилган сўзларнинг ушбу $T_{код}$ = {18, 1, 17, 5, 15, 17} кодларига эга бўламиз.

2-қадам.

Кодларга кўра, ушбу матрицаларни тузамиз:

$$B_1=\begin{vmatrix}18\\1\\17\end{vmatrix} \qquad B_2=\begin{vmatrix}5\\15\\17\end{vmatrix}$$

Энди T_1, T_2 матрицаларни топамиз. Бунинг учун $A*B_1$ ва $A*B_2$ лар учун ҳисоблашларни бажарамиз:

$$T_1=A*B_1=\begin{vmatrix}1&4&8\\3&7&2\\6&9&5\end{vmatrix}*\begin{vmatrix}18\\1\\17\end{vmatrix}=\begin{vmatrix}1*18+4*1+8*17\\3*18+7*1+2*17\\6*18+9*1+5*17\end{vmatrix}=\begin{vmatrix}18+4+136\\54+7+34\\108+9+85\end{vmatrix}=\begin{vmatrix}158\\95\\202\end{vmatrix}$$

$$T_2=A*B_2=\begin{vmatrix}1&4&8\\3&7&2\\6&9&5\end{vmatrix}*\begin{vmatrix}5\\15\\17\end{vmatrix}=\begin{vmatrix}1*5+4*15+8*17\\3*5+7*15+2*17\\6*5+9*15+5*17\end{vmatrix}=\begin{vmatrix}5+60+136\\15+105+34\\30+135+85\end{vmatrix}=\begin{vmatrix}201\\154\\250\end{vmatrix}$$

T = {T_1 U T_2 }= {158, 95, 202, 201, 154, 250}.

Жавоб: T_i = {САРДОР} = {158, 95, 202, 201, 154, 250}

Бу вазифанинг жавобини ифодалайди.

9.2.Хилл усули билан ахборотларни дешифрлаш

9. 2-вазифа.

Ушбу матрица кўринишда берилган

$$A=\begin{vmatrix}1&4&8\\3&7&2\\6&9&5\end{vmatrix}$$

калит билан T_i = {158, 95, 202, 201, 124, 250} кўринишдаги сонлар билан қандай сўз шифрланган?

Вазифанинг бажарилиши.

1-қадам. Берилган A матрицага тескари матрицани топамиз. Бунинг учун A матрицани детерминантини ҳисоблаймиз:

$$det\,(A)=\begin{vmatrix}1&4&8\\3&7&2\\6&9&5\end{vmatrix}=1*7*5+4*2*6+3*9*8-6*7*8-3*4*5-1*9*2=35+48+216-336-60-18=-115$$

2-3-қадам. Берилган A матрицага транспонирланган матрицани топамиз. Бунинг учун, даставвал қуйидаги матрицани тузамиз:

$$A^*=\begin{vmatrix}A_{11}&A_{12}&A_{13}\\A_{21}&A_{22}&A_{23}\\A_{31}&A_{32}&A_{33}\end{vmatrix}$$

Бу ерда A_{11}, A_{12}, ..., A_{33} лар A матрицанинг алгебраик тўлдирувчиларидир.

A матрицанинг алгебраик тўлдирувчиларини ҳисоблаймиз:

$$A_{11}=(-1)^{1+1}\begin{vmatrix} 7 & 2 \\ 9 & 5 \end{vmatrix} = (7*5-9*2)= (35-18) = 17.$$

$$A_{12}=(-1)^{1+2}\begin{vmatrix} 3 & 2 \\ 6 & 5 \end{vmatrix} = -(3*5-6*2)= -(15-12) = -3.$$

$$A_{13}=(-1)^{1+3}\begin{vmatrix} 3 & 7 \\ 6 & 9 \end{vmatrix} = (3*9 - 6*7) = (27 -42) = -15.$$

$$A_{21}=(-1)^{2+1}\begin{vmatrix} 4 & 8 \\ 9 & 5 \end{vmatrix} = -(4*5 - 9*8) = -(20 -72) = 52.$$

$$A_{22}=(-1)^{2+2}\begin{vmatrix} 1 & 8 \\ 6 & 5 \end{vmatrix} = (1*5 - 6*8) = (5 -48) = -43.$$

$$A_{23}=(-1)^{2+3}\begin{vmatrix} 1 & 4 \\ 6 & 9 \end{vmatrix} = -(1*9 - 6*4) = -(9 -24) = 15.$$

$$A_{31}=(-1)^{3+1}\begin{vmatrix} 4 & 8 \\ 7 & 2 \end{vmatrix} = (4*2 - 7*8) = (8 -56) = -48.$$

$$A_{32}=(-1)^{3+2}\begin{vmatrix} 1 & 8 \\ 3 & 2 \end{vmatrix} = -(1*2 - 3*8) = -(2 -24) = 22.$$

$$A_{33}=(-1)^{3+3}\begin{vmatrix} 1 & 4 \\ 3 & 7 \end{vmatrix} = (1*7 - 3*4) = (7 -12) = -5.$$

Юқорида ҳисобланганларни A^* га қуйиб қуйидагига эга бўламиз:

$$A^*=\begin{vmatrix} A_{11} & A_{12} & A_{13} \\ A_{21} & A_{22} & A_{23} \\ A_{31} & A_{32} & A_{33} \end{vmatrix} = \begin{vmatrix} 17 & -3 & -15 \\ 52 & -43 & 15 \\ -48 & 22 & -5 \end{vmatrix}$$

A^* матрицани транспонирлаб талаб қилинган A^T матрицага эга бўламиз:

$$A^T=\begin{vmatrix} A_{11} & A_{21} & A_{31} \\ A_{12} & A_{22} & A_{32} \\ A_{13} & A_{23} & A_{33} \end{vmatrix} = \begin{vmatrix} 17 & 52 & -48 \\ -3 & -43 & 22 \\ -15 & 15 & -5 \end{vmatrix}$$

2-3-қадам. Тескари A^{-1} матрицани ушбу формула билан топамиз:

$$A^{-1} = (1/\mathbf{det}\ (A))^* A^T$$

$$A^{-1} = (1/\det(A))^* A^T = (1/\det(A))^* \begin{vmatrix} A_{11} & A_{21} & A_{31} \\ A_{12} & A_{22} & A_{32} \\ A_{13} & A_{23} & A_{33} \end{vmatrix} = -(1/115)^* \begin{vmatrix} 17 & 52 & -48 \\ -3 & -43 & 22 \\ -15 & 15 & -5 \end{vmatrix}$$

4-қадам. Энди B_1 ва B_2 вектор матрицаларни аниқлаймиз.
Бу ерда қуйидаги формулларни қуллаймиз: $B_1 = A^{-1} * C_1$, $B_2 = A^{-1} * C_2$.

Энди вазифани берилишдаги T_i = {158, 95, 202, 201, 154, 250} сонлардан ушбу устун матрицаларини тузиб оламиз:

$$C_1 = \begin{vmatrix} 158 \\ 95 \\ 202 \end{vmatrix}; \qquad C_2 = \begin{vmatrix} 201 \\ 154 \\ 250 \end{vmatrix}.$$

$$B_1 = A^{-1} * C_1 = -(1/115)^* \begin{vmatrix} 17 & 52 & -48 \\ -3 & -43 & 22 \\ -15 & 15 & -5 \end{vmatrix} * \begin{vmatrix} 158 \\ 95 \\ 202 \end{vmatrix} = -(1/115)^* \begin{vmatrix} 17*158+52*95-48*202 \\ -3*158-43*95+22*202 \\ -15*158+15*95-5*202 \end{vmatrix} =$$

$$= -(1/115)^* \begin{vmatrix} 2686+4940-9696 \\ -474-4085+4444 \\ -2370+1425-1010 \end{vmatrix} = -(1/115)^* \begin{vmatrix} -2770 \\ -185 \\ -1955 \end{vmatrix} = \begin{vmatrix} 2770/115 \\ 185/115 \\ 1955/115 \end{vmatrix} = \begin{vmatrix} 18 \\ 1 \\ 17 \end{vmatrix}$$

$$B_2 = A^{-1} * C_2 = -(1/115)^* \begin{vmatrix} 17 & 52 & -48 \\ -3 & -43 & 22 \\ -15 & 15 & -5 \end{vmatrix} * \begin{vmatrix} 201 \\ 154 \\ 250 \end{vmatrix} = -(1/115)^* \begin{vmatrix} 17*201+52*154-48*250 \\ -3*201-43*154+22*250 \\ -15*201+15*154-5*250 \end{vmatrix} =$$

$$= -(1/115)^* \begin{vmatrix} 3417+8008-12000 \\ -603-6622+5500 \\ -3015+2310-1250 \end{vmatrix} = -(1/115)^* \begin{vmatrix} -575 \\ -1725 \\ -1955 \end{vmatrix} = \begin{vmatrix} 575/115 \\ 1725/115 \\ 1955/115 \end{vmatrix} = \begin{vmatrix} 5 \\ 15 \\ 17 \end{vmatrix}$$

Демак, қуйидаги матрицаларга эга бўлдик:

$$B_1 = \begin{vmatrix} 18 \\ 1 \\ 17 \end{vmatrix}; \qquad B_2 = \begin{vmatrix} 5 \\ 15 \\ 17 \end{vmatrix}.$$

Энди B_1 ва B_2 вектор устун матрицалардаги сонларни 1-жадвалда келтирилган ҳарфларнинг кодлари деб қараймиз, яъни:

$$B_1 = \begin{vmatrix} 18 \leftrightarrow \text{C} \\ 1 \leftrightarrow \text{A} \\ 17 \leftrightarrow \text{P} \end{vmatrix} \textit{ва} \quad B_2 = \begin{vmatrix} 5 \leftrightarrow \text{Д} \\ 15 \leftrightarrow \text{О} \\ 17 \leftrightarrow \text{P} \end{vmatrix}$$

ёки $T_{код}$ = {18,1,17,5,15,17} га эга бўлдик, бу сонларга 9.1-жадвалда келтирилаётган мос ҳарфларни қуйсак, изланаётган шифрланган сўзга эга бўламиз:

$T_{код}$ = {18,1,17,5,15,17} = {САРДОР}= $T_{матн}$

Саволлар ва жавоблар

1-савол. "САВОД" сўзидаги ҳарфларининг 9.1-жадвалга кўра кодлари қандай аниқланади?

Жавоб: $T_{матн}$ = {САВОД _ } = $T_{код}$ = {18,1,3,15,5,33}.

2-савол. "САДО" сўзидаги ҳарфларининг 9.1-жадвалга кўра кодлари қандай аниқланади?

Жавоб: $T_{матн}$ = { САДО_ _ } = $T_{код}$ = {18,1,5,3,33,33}.

3-савол. "САВОДСИЗ" сўзидаги ҳарфларининг 9.1-жадвалга кўра кодларидан қандай устун матрицалар тузилади?

Изоҳ. Калит ўлчами (3:3) дан иборат матрица бўлсин, масалан:

$$A=\begin{vmatrix} 4 & 5 & 6 \\ 8 & 3 & 2 \\ 9 & 7 & 1 \end{vmatrix}$$

Жавоб: $T_{матн}$ = {САВОДСИЗ} = $T_{код}$ = {18,1,3,15,5,18,9,8}.

Кодларга кўра, ушбу матрицалар тузилади: $B_1=\begin{vmatrix} 18 \\ 1 \\ 3 \end{vmatrix}$ $B_2=\begin{vmatrix} 15 \\ 5 \\ 18 \end{vmatrix}$ $B_2=\begin{vmatrix} 9 \\ 8 \\ 33 \end{vmatrix}$

Амалий машғулот вазифалари

I.Дарснинг мақсади. Талабаларга ахборот ҳимояси ва хавфсизлигида шифрлашнинг аналитик усуллари ҳисобланган Хилл усули билан ахборотларни шифрлаш ва дешифрлашни ўргатиш.

II. Информацион техник ва услубий воситалар

II.1. Pentium компьютерлари, кадоскоп, видеоплеер ва плакатлар

II.2. Адабиётлар: [1, 2, 3, 4, 5, 6, 7] ва мавзу бўйича тарқатма материалллар

9.1.1-вазифа.

1)$T_{матн}$ = {АНВАРА} сўзини ушбу калит- матрица билан шифрланг $A=\begin{vmatrix}1&4&8\\3&7&2\\6&9&5\end{vmatrix}$

2) Шифрланган сўзни тескари матрица тузиш орқали очинг

9.1.2- вазифа.

1)$T_{матн}$ = {БИЗНЕС} сўзини ушбу калит- матрица билан шифрланг $A=\begin{vmatrix}1&4&8\\3&7&2\\6&9&5\end{vmatrix}$

2) Шифрланган сўзни тескари матрица тузиш орқали очинг

9.1.3- вазифа.

1)$T_{матн}$ = {МАРКЕТ} сўзини ушбу калит- матрица билан шифрланг $A=\begin{vmatrix}1&4&8\\3&7&2\\6&9&5\end{vmatrix}$

2) Шифрланган сўзни тескари матрица тузиш орқали очинг

9.1.4- вазифа.

1)$T_{матн}$ = {НАРВОН} сўзини ушбу калит- матрица билан шифрланг $A=\begin{vmatrix}1&4&8\\3&7&2\\6&9&5\end{vmatrix}$

2) Шифрланган сўзни тескари матрица тузиш орқали очинг

9.1.5- вазифа.

1)$T_{матн}$ = {КАРВОН} сўзини ушбу калит- матрица билан шифрланг $A=\begin{vmatrix}1&4&8\\3&7&2\\6&9&5\end{vmatrix}$

2) Шифрланган сўзни тескари матрица тузиш орқали очинг

9.1.6- вазифа.

1)$T_{матн}$ = {БОЗОР_ } сўзини ушбу калит- матрица билан шифрланг $A=\begin{vmatrix}1&4&8\\3&7&2\\6&9&5\end{vmatrix}$

2) Шифрланган сўзни тескари матрица тузиш орқали очинг

9.1.7- вазифа.

1)$Т_{матн}$ = {ОФТОБ_} сўзини ушбу калит- матрица билан шифрланг $A=\begin{vmatrix}1&4&8\\3&7&2\\6&9&5\end{vmatrix}$

2) Шифрланган сўзни тескари матрица тузиш орқали очинг

9.1.8- вазифа.

1)$Т_{матн}$ = {НИГОРА} сўзини ушбу калит- матрица билан шифрланг $A=\begin{vmatrix}1&4&8\\3&7&2\\6&9&5\end{vmatrix}$

2) Шифрланган сўзни тескари матрица тузиш орқали очинг

9.1.9- вазифа.

1)$Т_{матн}$ = {ДИЛБАР} сўзини ушбу калит- матрица билан шифрланг $A=\begin{vmatrix}1&4&8\\3&7&2\\6&9&5\end{vmatrix}$

2) Шифрланган сўзни тескари матрица тузиш орқали очинг

9.1.10- вазифа.

1)$Т_{матн}$ = {МАКСУД} сўзини ушбу калит- матрица билан шифрланг $A=\begin{vmatrix}1&4&8\\3&7&2\\6&9&5\end{vmatrix}$

2) Шифрланган сўзни тескари матрица тузиш орқали очинг

9.1.11- вазифа.

1)$Т_{матн}$ = {КАФЕДР} сўзини ушбу калит- матрица билан шифрланг $A=\begin{vmatrix}1&4&8\\3&7&2\\6&9&5\end{vmatrix}$

2) Шифрланган сўзни тескари матрица тузиш орқали очинг

9.1.12- вазифа.

1)$Т_{матн}$ = {МАНЗУР} сўзини ушбу калит- матрица билан шифрланг $A=\begin{vmatrix}1&4&8\\3&7&2\\6&9&5\end{vmatrix}$

2) Шифрланган сўзни тескари матрица тузиш орқали очинг

9.1.13- вазифа.

1)$Т_{матн}$ = {БОЛА_ _} сўзини ушбу калит- матрица билан шифрланг $A=\begin{vmatrix}1&4&8\\3&7&2\\6&9&5\end{vmatrix}$

2) Шифрланган сўзни тескари матрица тузиш орқали очинг

9.1.14- вазифа.

1)$Т_{матн}$ = {ТАЛАБА} сўзини ушбу калит- матрица билан шифрланг $A=\begin{vmatrix}1&4&8\\3&7&2\\6&9&5\end{vmatrix}$

2) Шифрланган сўзни тескари матрица тузиш орқали очинг

Лаборатория иши вазифалари

I.**Дарснинг мақсади.** Лаборатория ишларида талабаларга ахборот хавфсизлиги ва ҳимоясида шифрлашнинг аналитик усуллари ҳисобланган Хилл усули билан ахборотларни шифрлаш ва дешифрлашни мустақил бажаришни ўргатиш.

II. Информацион техник ва услубий воситалар

II.1. Pentium компьютерлари, кадоскоп, видеоплеер ва плакатлар

II.2. Адабиётлар: [1, 2, 3, 4, 5, 6, 7] ва мавзу бўйича тарқатма материалллар

9.2.1-Вариант.

1)$T_{матн}$ = {АНВАРА} сўзини ушбу калит- матрица билан шифрланг $A=\begin{vmatrix} 2 & 1 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{vmatrix}$

2) Шифрланган сўзни тескари матрица тузиш орқали очинг

9.2.2-Вариант.

1)$T_{матн}$ = {БИЗНЕС} сўзини ушбу калит- матрица билан шифрланг $A=\begin{vmatrix} 3 & 2 & 1 \\ 6 & 5 & 4 \\ 7 & 8 & 9 \end{vmatrix}$

2) Шифрланган сўзни тескари матрица тузиш орқали очинг

9.2.3-Вариант.

1)$T_{матн}$ = {МАРКЕТ} сўзини ушбу калит- матрица билан шифрланг $A=\begin{vmatrix} 6 & 3 & 2 \\ 1 & 5 & 4 \\ 8 & 7 & 9 \end{vmatrix}$

2) Шифрланган сўзни тескари матрица тузиш орқали очинг

9.2.4-Вариант.

1)$T_{матн}$ = {НАРВОН} сўзини ушбу калит- матрица билан шифрланг $A=\begin{vmatrix} 4 & 1 & 2 \\ 3 & 5 & 6 \\ 7 & 8 & 9 \end{vmatrix}$

2) Шифрланган сўзни тескари матрица тузиш орқали очинг

9.2.5-Вариант.

1)$T_{матн}$ = {КАРВОН} сўзини ушбу калит- матрица билан шифрланг $A=\begin{vmatrix} 3 & 6 & 5 \\ 4 & 1 & 2 \\ 8 & 7 & 9 \end{vmatrix}$

2) Шифрланган сўзни тескари матрица тузиш орқали очинг

9.2.6-Вариант.

1)$T_{матн}$ = {БОЗОР } сўзини ушбу калит- матрица билан шифрланг $A=\begin{vmatrix} 6 & 5 & 3 \\ 4 & 1 & 2 \\ 8 & 7 & 9 \end{vmatrix}$

2) Шифрланган сўзни тескари матрица тузиш орқали очинг

9.2.7-Вариант.

1)$T_{матн}$ = {ОФТОБ} сўзини ушбу калит- матрица билан шифрланг $A=\begin{vmatrix} 1 & 2 & 4 \\ 3 & 5 & 6 \\ 9 & 7 & 8 \end{vmatrix}$

2) Шифрланган сўзни тескари матрица тузиш орқали очинг

9.2.8-Вариант.

1)$T_{матн}$ = {НИГОРА} сўзини ушбу калит- матрица билан шифрланг $A=\begin{vmatrix} 4 & 1 & 8 \\ 3 & 7 & 2 \\ 6 & 9 & 5 \end{vmatrix}$

2) Шифрланган сўзни тескари матрица тузиш орқали очинг

9.2.9.-Вариант.

1)$T_{матн}$ = {ДИЛБАР} сўзини ушбу калит- матрица билан шифрланг $A=\begin{vmatrix} 6 & 1 & 8 \\ 3 & 7 & 2 \\ 4 & 9 & 5 \end{vmatrix}$

2) Шифрланган сўзни тескари матрица тузиш орқали очинг

9.2.10- Вариант.

1)$T_{матн}$ = {МАКСУД} сўзини ушбу калит- матрица билан шифрланг $A=\begin{vmatrix} 7 & 1 & 8 \\ 3 & 6 & 2 \\ 4 & 9 & 5 \end{vmatrix}$

2) Шифрланган сўзни тескари матрица тузиш орқали очинг

9.2.11-Вариант.

1)$T_{матн}$ = {КАФЕДР} сўзини ушбу калит- матрица билан шифрланг $A=\begin{vmatrix} 5 & 1 & 8 \\ 3 & 6 & 2 \\ 4 & 9 & 7 \end{vmatrix}$

2) Шифрланган сўзни тескари матрица тузиш орқали очинг

9.2.12-вариант.

1)$T_{матн}$ = {МАНЗУР} сўзини ушбу калит- матрица билан шифрланг $A=\begin{vmatrix} 5 & 4 & 8 \\ 3 & 6 & 2 \\ 1 & 9 & 7 \end{vmatrix}$

2) Шифрланган сўзни тескари матрица тузиш орқали очинг

9.2.13-вариант.

1)$T_{матн}$ = {БОЛА} сўзини ушбу калит- матрица билан шифрланг $A=\begin{vmatrix} 5 & 4 & 6 \\ 3 & 8 & 2 \\ 7 & 1 & 9 \end{vmatrix}$

2) Шифрланган сўзни тескари матрица тузиш орқали очинг

2) Шифрланган сўзни тескари матрица тузиш оркали очинг.
3) Бажарилган ишларни таснифланг.

9.3.5 - вариант.

1)$T_{матн}$ = {фамилия, исм} матнни билан шифрланг $A=\begin{vmatrix} 1 & 4 & 8 \\ 2 & 3 & 7 \\ 6 & 9 & 5 \end{vmatrix}$ калит- матрица

2) Шифрланган сўзни тескари матрица тузиш оркали очинг.
3) Бажарилган ишларни таснифланг.

9.3.6 - вариант.

1)$T_{матн}$ = {фамилия, исм} матнни билан шифрланг $A=\begin{vmatrix} 4 & 2 & 1 \\ 5 & 3 & 6 \\ 7 & 8 & 9 \end{vmatrix}$ калит- матрица

2) Шифрланган сўзни тескари матрица тузиш оркали очинг.
3) Бажарилган ишларни таснифланг.

9.3.7 - вариант.

1)$T_{матн}$ = {фамилия, исм} матнни билан шифрланг $A=\begin{vmatrix} 8 & 1 & 6 \\ 7 & 3 & 2 \\ 4 & 5 & 9 \end{vmatrix}$ калит- матрица

2) Шифрланган сўзни тескари матрица тузиш оркали очинг.
3) Бажарилган ишларни таснифланг.

9.3.8 - вариант.

1)$T_{матн}$ = {фамилия, исм} матнни билан шифрланг $A=\begin{vmatrix} 5 & 6 & 3 \\ 4 & 2 & 1 \\ 7 & 9 & 8 \end{vmatrix}$ калит- матрица

2) Шифрланган сўзни тескари матрица тузиш оркали очинг.
3) Бажарилган ишларни таснифланг.

9.3.9 - вариант.

1)$T_{матн}$ = {фамилия, исм} матнни билан шифрланг $A=\begin{vmatrix} 3 & 5 & 6 \\ 2 & 4 & 1 \\ 8 & 7 & 9 \end{vmatrix}$ калит- матрица

2) Шифрланган сўзни тескари матрица тузиш оркали очинг.
3) Бажарилган ишларни таснифланг.

9.3.10 - вариант.

1)$T_{матн}$ = {фамилия, исм} матнни билан шифрланг $A=\begin{vmatrix} 2 & 1 & 4 \\ 5 & 6 & 3 \\ 8 & 7 & 9 \end{vmatrix}$ калит- матрица

2) Шифрланган сўзни тескари матрица тузиш оркали очинг.
3) Бажарилган ишларни таснифланг.

9.3.11 - вариант.

1)$T_{матн}$ = {фамилия, исм} матнни билан шифрланг $A=\begin{vmatrix} 5 & 4 & 6 \\ 3 & 8 & 2 \\ 7 & 1 & 9 \end{vmatrix}$ калит- матрица

2) Шифрланган сўзни тескари матрица тузиш оркали очинг.
3) Бажарилган ишларни таснифланг.

9.3.12 - вариант.

1)$T_{матн}$ = {фамилия, исм} матнни билан шифрланг $A=\begin{vmatrix} 2 & 3 & 6 \\ 1 & 5 & 4 \\ 7 & 8 & 9 \end{vmatrix}$ калит- матрица

2) Шифрланган сўзни тескари матрица тузиш орқали очинг.

3) Бажарилган ишларни таснифланг.

9.3.13 - вариант.

1)$T_{матн}$ = {фамилия, исм} матнни билан шифрланг $A=\begin{vmatrix} 6 & 2 & 3 \\ 5 & 1 & 4 \\ 8 & 9 & 7 \end{vmatrix}$ калит- матрица

2) Шифрланган сўзни тескари матрица тузиш орқали очинг.

3) Бажарилган ишларни таснифланг.

9.3.14 - вариант.

1)$T_{матн}$ = {фамилия, исм} матнни билан шифрланг $A=\begin{vmatrix} 6 & 2 & 3 \\ 4 & 1 & 5 \\ 8 & 7 & 9 \end{vmatrix}$ калит- матрица

2) Шифрланган сўзни тескари матрица тузиш орқали очинг.

3) Бажарилган ишларни таснифланг.

9.3.15 - вариант.

1)$T_{матн}$ = {фамилия, исм} матнни билан шифрланг $A=\begin{vmatrix} 2 & 6 & 3 \\ 5 & 7 & 4 \\ 8 & 9 & 1 \end{vmatrix}$ калит- матрица

2) Шифрланган сўзни тескари матрица тузиш орқали очинг.

3) Бажарилган ишларни таснифланг.

9.3.16 - вариант.

1)$T_{матн}$ = {фамилия, исм} матнни билан шифрланг $A=\begin{vmatrix} 6 & 2 & 3 \\ 5 & 4 & 1 \\ 7 & 9 & 8 \end{vmatrix}$ калит- матрица

2) Шифрланган сўзни тескари матрица тузиш орқали очинг.

3) Бажарилган ишларни таснифланг.

9.3.17 - вариант.

1)$T_{матн}$ = {фамилия, исм} матнни билан шифрланг $A=\begin{vmatrix} 6 & 7 & 5 \\ 3 & 1 & 4 \\ 8 & 9 & 2 \end{vmatrix}$ калит- матрица

2) Шифрланган сўзни тескари матрица тузиш орқали очинг.

3) Бажарилган ишларни таснифланг.

9.3.18 - вариант.

1)$T_{матн}$ = {фамилия, исм} матнни билан шифрланг $A=\begin{vmatrix} 6 & 2 & 3 \\ 9 & 1 & 4 \\ 8 & 5 & 7 \end{vmatrix}$ калит- матрица

2) Шифрланган сўзни тескари матрица тузиш орқали очинг.

3) Бажарилган ишларни таснифланг.

9.3.19 - вариант.

1)$T_{матн}$ = {фамилия, исм} матнни билан шифрланг $A=\begin{vmatrix} 6 & 5 & 3 \\ 2 & 1 & 4 \\ 8 & 7 & 9 \end{vmatrix}$ калит- матрица

Мустақил таълим учун материаллар[3]

Мавзу. Вирусларнинг файллар таркибига таъсири

1.Файллар таркибини бузувчи ва бузмайдиган вируслар

2. Оператор ва қурилмаларга таъсир қилувчи вируслар

Файллар таркибини бузувчи ва бузмайдиган вируслар

Вируслар асосан дискларнинг юкланувчи секторларини ва **exe**, **com**, **sys** ва **bat** кенгайтмали файлларни зарарлайди. Ҳозирги кунда булар қаторига офис дастурлари яратадиган файлларни ҳам киритиш мумкин. Оддий матнли файлларни зарарлайдиган вируслар камдан-кам учрайди.

Файллар таркибини бузмайдиган вируслар: оператив хотира қурилмасида кўпаювчи; операторни таъсирлантирувчи; тармоқ вируслари

Операторни таъсирлантирувчи			
Қурилмаларни ишдан чиқарувчи	Терминалда хабар чиқарувчи	Товушли эффектларни ҳосил қилувчи	Иш тартибини ўзгартирувчи
Процессор			Клавиатура
Хотира	Матнли	Оҳанг	
МД, винчестер			Дисплей
Принтер	Графикли	Нутқ синтези	
Порт PS-232			Принтер
Дисплей		Махсус эффектли	
Клавиатура			Порт PS-232

Компьютернинг вируслар билан зарарланиш йўллари қуйидагилардир:

1.Дискетлар орқали.2. Компьютер тармоқлари орқали.

2.Бошқа йўллар йўқ.

Файл таркибини бузувчи вируслар:				
Фойдаланувчининг маълумотлари ва дастурларини бузувчи		**Тизим маълумотларини бузувчи**		
Дастурларни бузувчи	Маълумотларни бузувчи	Диск соҳасини бузувчи	Форматлаш	Тизкор Тизим Файлларини бузувчи
Бажариладиган дастурларни бузувчи	Маълумотлар базаларини бузувчи			
Компиляторларнинг қисм дастурлар тўпламини бузувчи	График тасвирни бузувчи			

[3] Мустақил таълим мавзулари «Алимов Р.Х, Ходиев Б.Ю., Алимов Қ. А., Усмонов С.У., Бегалов Б.Б., Зайналов Н.Р., Мусалиев А.А., Файзиева Ф. Миллий иқтисодда ахборот тизимлари ва технологиялари. «Шарқ». Тошкент. 2004» дан келтирилмоқда.

қийинчиликларга олиб келади. **Мутант вирус** - шифрлаш ва дешифрлаш алгоритмларидан иборат бўлиб, натижада вирус нусхалари умуман бир-бирига ўхшамайди. Ушбу вирусларни аниқлаш жуда қийин муаммо ҳисобланади.**Квазивирус вирус** - «Троян» дастурлари, деб ном олган бўлиб, ушбу вируслар кўпайиш хусусиятига эга бўлмасада, «фойдали» қисм-дастур ҳисобида бўлиб, антивирус дастурлар томонидан аниқланмайди. Шу боис ҳам улар ўзларида мукаммаллаштирилган алгоритмларни тўсиқсиз бажариб, қуйилган мақсадларига эришишлари мумкин.

Мавзу. Ташкилотларда ахборотларни ҳимоялаш

1. Ташкилотларда ахборотларни ҳимоялаш
2.Ахборотларни ташкилий ҳимоялаш элементлари
3. Ахборот тизимларида маълумотларга нисбатан хавф-хатарлар

Ташкилотлардаги ахборотларни ҳимоялаш

Ахборот ҳажми кичик бўлган ташкилотларда ахборотларни ҳимоялашда оддий усулларни қўллаш мақсадга мувофиқ ва самаралидир. Масалан, ўқиладиган қимматбаҳо қоғозларни ва электрон ҳужжатларни алоҳида гуруҳларга ажратиш ва никоблаш, ушбу ҳужжатлар билан ишлайдиган ходимни тайинлаш ва ўргатиш, бинони қўриқлашни ташкил этиш, хизматчиларга қимматли ахборотларни тарқатмаслик мажбуриятини юклаш, ташқаридан келувчилар устидан назорат қилиш, компьютерни ҳимоялашнинг энг оддий усулларини қўллаш ва ҳоказо. Одатда, ҳимоялашнинг энг оддий усулларини қўллаш сезиларли самара беради.

Мураккаб таркибли, кўп сонли автоматлаштирилган ахборот тизими ва ахборот ҳажми катта бўлган ташкилотларда ахборотни ҳимоялаш учун ҳимоялашнинг мажмуали тизими ташкил қилинади. Лекин ушбу усул ҳамда ҳимоялашнинг оддий усуллари хизматчиларнинг ишига ҳаддан ташқари ҳалақит бермаслиги керак.

Ахборотларни ташкилий ҳимоялаш элементлари

Ҳимоялаш технологияси персонални ташкилотнинг қимматли ахборотларини ҳимоялаш қоидаларига риоя қилишга ундовчи бошқариш ва чеклаш характерига эга бўлган чора-тадбирларни ўз ичига олади.

Ташкилий ҳимоялаш элементи бошқа барча элементларни ягона тизимга боғловчи омил бўлиб ҳисобланади. Кўпчилик мутахассисларнинг фикрича, ахборотларни ҳимоялаш тизимлари таркибида ташкилий ҳимоялаш 50—60 фоизни ташкил қилади, Бу ҳол кўп омилларга боғлиқ, жумладан, ахборотларни ташкилий ҳимоялашнинг асосий томони амалда ҳимоялашнинг принципи ва усулларини бажарувчи персонални танлаш, жойлаштириш ва ўргатиш ҳисобланади.

Ахборотларни ҳимоялашнинг ташкилий чора-тадбирлари ташкилот хавфсизлиги хизматнинг меъёрий услубий ҳужжатларида ўз аксини топади. Шу муносабат билан кўп ҳолларда юқорида кўрилган тизим элементларининг ягона номи- ахборотни ташкилий-хуқуқий ҳимоялаш элементини ишлатадилар.

Ахборотларни муҳандис-техник ҳимоялаш элементи-техник воситалар комплекси ёрдамида худуд, бино ва қурилмаларни қўриқлашни ташкил қилиш

ҳамда техник текшириш воситаларига қарши суст ва фаол курaш учун мўлжалланган. Техник ҳимоялаш воситаларининг нархи баланд бўлсада, ахборот тизимини ҳимоялашда бу элемент муҳим аҳамиятга эга.

Ахборотни ҳимоялашнинг дастурий-математик элементи компьютер, локал тармоқ ва турли ахборот тизимларида қайта ишланадиган ва сақланадиган қимматли ахборотларни ҳимоялаш учун мўлжалланган.

Ахборот тизимларида маълумотларга нисбатан хавф –хатарлар

Компьютер тизими (тармоғи)га зиён етказиши мумкин бўлган шароит, ҳаракат ва жараёнлар **компьютер тизими (тармоғи) учун хавф-хатарлар,** деб ҳисобланади.

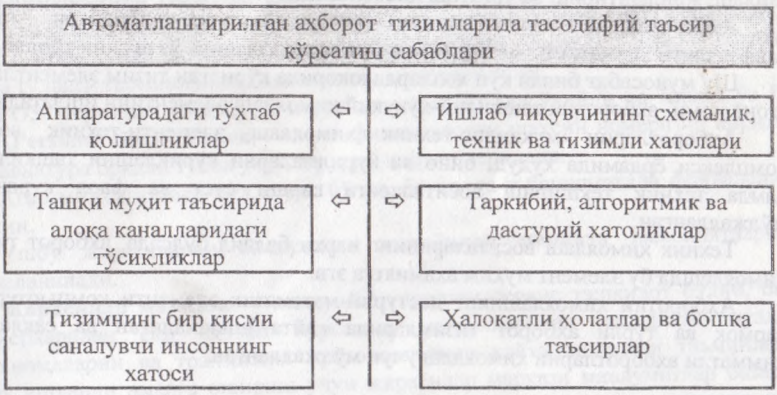
Автоматлаштирилган ахборот тизимларига тасодифий таъсир кўрсатиш сабаблари таркибига қуйидагилар киради.

Маълумки, компьютер тизим (тармоғ)ининг асосий компонентлари - техник воситалари, дастурий-математик таъминот ва маълумотлардир.

Назарий томондан бу компонентларга нисбатан тўрт турдаги хавфлар мавжуд, яъни узилиш, **тутиб қолиш, ўзгартириш ва сохталаштириш:**

Узилиш-қандайдир ташки ҳаракатлар (ишлар, жараёнлар)ни бажариш учун ҳозирги ишларни вақтинча марказий процессор қурилмаси ёрдамида тўхтатишдир, уларни бажаргандан сўнг процессор оддинги ҳолатга қайтади ва тўхтатиб қўйилган ишни давом эттиради. Ҳар бир узилиш тартиб рақамига эга, унга асосан марказий процессор қурилмаси қайта ишлаш учун қисм дастурни кидириб топади. Процессорлар икки турдаги узилишлар билан ишлашни вужудга келтириши мумкин: дастурий ва техник.

Бирор қурилма фавқулодда хизмат кўрсатилишига муҳтож бўлса, унда техник узилиш пайдо бўлади. Одатда бундай узилиш марказий процессор учун кутилмаган ҳодисадир. Дастурий узилишлар асосий дастурлар ичида процессорнинг махсус буйруклари ёрдамида бажарилади. Дастурий узилишда дастур ўз-ўзини вақтинча тўхтатиб, узилишга тааллукли жараённи бажаради.



Автоматлаштирилган ахборот тизимларига тасодифий таъсир кўрсатиш сабаблари:

• **тутиб олиш** — жараёни окибатида ғаразли шахслар дастурий воситалар ва ахборотларнинг турли магнитли ташувчиларига киришни қўлга киритади. Дастур ва маълумотлардан ноқонуний нусха олиш, компьютер тармоклари алоқа каналларидан номуаллифлик ўқишлар ва ҳоказо ҳаракатлар тутиб олиш жараёнларига мисол бўла олади;

• **ўзгартириш** - ушбу жараён ёвуз ниятли шахс нафақат компьютер тизими компонентларига (маълумотлар тўпламлари, дастурлар, техник элементлари) киришни қўлга киритади, балки улар билан манипуляция (ўзгартириш, кўринишини ўзгартириш) ҳам қилади. Масалан, ўзгартириш сифатида ғаразли шахснинг маълумотлар тўпламидаги маълумотларни ўзгартириши, ёки умуман компьютер тизими файлларини ўзгартириши, ёки қандайдир қўшимча ноқонуний қайта ишлашни амалга ошириш мақсадида фойдаланилаётган дастурнинг кодини ўзгартириши тушунилади;

• **сохталаштириш** - ҳам жараён саналиб, унинг ёрдамида ғаразли шахслар тизимда ҳисобга олинмаган вазиятларни ўрганиб, ундаги камчиликларни аниқлаб, кейинчалик ўзига керакли ҳаракатларни бажариш мақсадида тизимга қандайдир сохта жараённи ёки тизим ва бошқа фойдаланувчиларга сохта ёзувларни юборади.

Ахборотларни ташкилий ҳимоялаш элементлари

Ҳимоялаш технологияси персонални ташкилотнинг қимматли ахборотларини ҳимоялаш қоидаларига риоя қилишга ундовчи бошқариш ва чеклаш характерига эга бўлган чора-тадбирларни ўз ичига олади.

Ташкилий ҳимоялаш элементи бошқа барча элементларни ягона тизимга боғловчи омил бўлиб ҳисобланади.

Кўпчилик мутахассисларнинг фикрича, ахборотларни ҳимоялаш тизимлари таркибида ташкилий ҳимоялаш 50—60 фоизни ташкил қилади, Бу ҳол кўп омилларга боғлиқ, жумладан, ахборотларни ташкилий ҳимоялашнинг асосий томони амалда ҳимоялашнинг принципи ва усулларини бажарувчи персонални танлаш, жойлаштириш ва ўргатиш ҳисобланади.

Ахборотларни ҳимоялашнинг ташкилий чора-тадбирлари ташкилот хавфсизлиги хизматнинг меъёрий услубий ҳужжатларида ўз аксини топади.

Шу муносабат билан кўп ҳолларда юқорида кўрилган тизим элементларининг ягона номи- ахборотни ташкилий-ҳуқуқий ҳимоялаш элементини ишлатадилар.

Ахборотларни муҳандис-техник ҳимоялаш элементи-техник воситалар комплекси ёрдамида ҳудуд, бино ва қурилмаларни кўриқлашни ташкил қилиш ҳамда техник текшириш воситаларига қарши суст ва фаол кураш учун мўлжалланган.

Техник ҳимоялаш воситаларининг нархи баланд бўлсада, ахборот тизимини ҳимоялашда бу элемент муҳим аҳамиятга эга.

Ахборотни ҳимоялашнинг дастурий-математик элементи компьютер, локал тармоқ ва турли ахборот тизимларида қайта ишланадиган ва сақланадиган қимматли ахборотларни ҳимоялаш учун мўлжалланган.

Мавзу. Электрон тўловлар тизимида ахборотларни ҳимоялаш

1. Электрон тўловлар тизими
2. Идентификация шахсий номерини ҳимоялаш
3. Банкоматлар хавфсизлигини таъминлаш
4. Интернетда мавжуд электрон туловлар хавфсизлини таъминлаш
Ахборотларни ҳимоялаш воситалари

Электрон тўловлар тизими асослари

Электрон тўловлар тизими деб банк пластик карталарини тўлов воситаси сифатида қўлланилишидаги усуллар ва уларни амалга оширувчи субъектлар мажмуасига айтилади.

Пластик карта- шахсий тўлов воситаси бўлиб, у мазкур воситадан фойдаланадиган шахсга товар ва хизматларни нақдсиз пулини тўлаш, бундан ташқари банк муассасалари ва банкоматлардан нақд пулни олишга имкон беради.

Пластик картани тўлов воситаси сифатида қабул қилувчилар, савдо ва хизмат кўрсатувчи корхоналар, банк бўлимлари ҳамда бошқалар шу пластик карталарга хизмат кўрсатувчи қабул килувчилар тармоғини ташкил этади.

Электрон тўловлар тизимини яратишда пластик карталарга хизмат кўрсатиш конунини қоидаларини ишлаб чиқиш ва уларга риоя қилиш асосий масалалардан бири бўлиб ҳисобланади. Ушбу қоидалар нафақат техникавий (маълумотларни стандартлаш, ускуналар ва бошқалар), балки молиявий масалалар (корхоналар билан ҳисобларни бажариш тартиби)ни ҳам қамраб олади.

Электрон тўловлар тизими билан биргаликда фаолият кўрсатадиган банк икки, яъни **банк-эмитент ва банк-эквайер** тоифасида хизмат кўрсатади:

Банк-эмитент пластик карталарни ишлаб чиқаради ва уларнинг тўлов воситаси сифатида қўлланилишига кафолат беради.

Банк-эквайер савдо ва хизмат кўрсатувчи ташкилотлар томонидан қабул қилинган тўловларни банк бўлимлари ёки банкоматлар орқали амалга оширади.

Ҳозирги кунда автоматлаштирилган савдо **POS** (Point –Of-Sale — сотилган жойда тўлаш)- терминали ва банкоматлар кенг тарқалган.

POS -терминалда пластик картадан маълумотлар ўқийди ва мижоз ўз **PIN** коди (**Personal Identification** - идентификацияловчи шахсий номери)ни киритади ва клавиатура орқали тўлов учун зарурий қиймат терилади.

Агар мижозга нақд пул керак бўлса, бу ҳолда у банкоматдан фойдаланиши мумкин.

Ушбу жараёнларни бажаришда **жараёнлар маркази** имкониятларидан фойдаланилади.

Жараёнлар маркази - махсуслаштирилган сервис ташкилот бўлиб, банк-эквайерларидан ёки хизмат кўрсатиш манзилларидан келадиган муаллиф сўровномаларни ва транзакция протоколларини қайта ишлашни таъминлайди. Ушбу ишларни амалга ошириш учун жараёнлар маркази маълумотлар базасини киритади. Бу маълумотлар базаси тўлов тизими, банк аъзолари ва пластик карта соҳиблари тўғрисидаги маълумотларни ўз таркибига олади.

Пластик карталар тўлов бўйича **кредитли ёки дебетли** бўлиши мумкин.

Кредитли карталар бўйича карта соҳибига кўпинча муҳлати 25 кунгача бўлган вақтинча қарз берилади. Буларга **Visa, Master Card, American Express** карталари мисол бўла олади.

Дебетли карталарда карта соҳибининг банк-эмитентидаги ҳисобига олдиндан маълум миқдорда маблағ жойлаштиради. Ушбу маблағдан харид учун ишлатилган маблағлар суммаси ошиб кетмаслиги лозим.

Ушбу карталар фақатгина шахсий эмас, балки корпоратив ҳам бўлиши мумкин.

Хозирги кунда **микропроцессорли карталар** ишлаб чиқилмоқда. Ушбу карталарнинг олдингиларидан асосий фарқи бу мижознинг барча маълумотлари унда акс эттирилган бўлиб, барча **транзакциялар,** яъни маълумотлар базасини бир ҳолатдан иккинчи ҳолатга ўтказувчи сўровномалар, **off-line** режимда амалга оширилади, шу боис, улар юқори даражада ҳимояланган деб эътироф этилган. Уларнинг нархи қимматроқ бўлсада, телекоммуникация каналларидан фойдаланилмаслик муносабати билан ундан фойдаланиш қиймати арзондир.

Электрон тўлов тизимларининг қуйидаги заиф қисмлари мавжуд:

банк ва мижоз, банкларарo, банк ва банкомат орасида тўлов маълумотларини жўнатиш; ташкилот доирасида маълумотларни кайта ишлаш.

Булар уз навбатида қуйидаги муаммоларни юзага келтиради: абоиснтларнинг хақиқийлигини аниклаш; алоқа каналлари орқали жўнатилаётган электрон хужжатларнн ҳимоялаш; электрон хужжатларининг юборилганлигига ва қабул кдпинганлигига ишонч ҳосил қилиш; хужжатнинг бажарилишини таъминлаш.

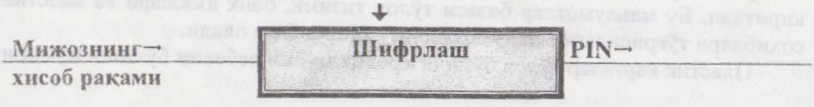
Электрон тўловлар тизимида ахборотларни ҳимоялаш функцияларини таъминлаш мақсадида қуйидагилар амалга оширилиши керак: тизимнинг четки бутинларига киришни бошк.а риш; ахборотларнинг яхлитлигини назорат к.илиш; хабарларнинг махфийлигини таъминлаш; абонентларни ўзаро аутентификациялаш; хабарнинг муаллифлигидан воз кеча олмаслик; хабарнинг етказилганлигини кафолатлаш; хабар бўйича бажариладиган чора-тадбирлардан воз кеча олмаслик; хабарлар кетма-кетлигини қайд қилиш; кетма-кет хабарлар яхлитлигини таъминлаш.

Идентификацияловчи шахсий номерни ҳимоялаш

PIN -кодларини ҳимоялаш тўлов тизими хавфсизлигини таъминлашда асосий омилдир. Шу боис у фақатгина карта соҳибига маълум бўлиб, электрон тўловлар тизимида сақланмайди ва бу тизим бўйича юборилмайди.

Умуман олганда, **PIN** банк томонидан берилиши ёки мижоз томонидан танланиши мумкин. Банк томонидан бериладиган **PIN** қуйидаги икки вариантдан бири бўйича амалга оширилади:

1)мижоз ҳисоб рақами бўйича криптография усули билан ташкиллаштирилади;



Ушбу усулнинг афзаллиги **PIN** коди электрон тўловлар тизимида сақланиши шарт эмаслигидадир, камчилиги эса ушбу мижоз учун бошқа PIN берилиши лозим бўлса, унга бошқа ҳисоб рақами очилиши зарурлигида, чунки банк бўйича битта калит қўлланилади.

2) банк ихтиёрий **PIN** кодни таклиф қилади ва уни ўзида шифрлаб сақлайди. **PIN** кодни хотирада сақлаш қийинлиги ушбу усулнинг асосий камчилиги бўлиб ҳисобланади.

Мижоз томонидан танланиладиган PIN код қуйидаги имкониятларга эга:

- барча мақсадлар учун ягона PIN кодни қўллаш;
- ҳарфлар ва рақамлардан ташкил этилган PIN кодни хотирада сақлашнинг енгиллиги.

PIN коди бўйича мижозни идентификациялаштиришнинг икки усули билан бажариш мумкин: **алгоритмлашган ва алгоритмлашмаган.**

Алгоритмлашмаган текшириш усулида элемент киритган PIN код маълумотлар базасидаги шифрланган код билан таққосланилади.

Алгоритмлашган текшириш усулида эса мижоз киритган PIN код, махфий калитдан фойдаланган ҳолда, махсус алгоритм бўйича ўзгартирилади ва картадаги ёзув билан таққосланилади.

Ушбу усулнинг афзалликлари: асосий компьютерда PIN сақланмайди ва натижада персонал томонидан ўғирланмайди; PIN код телекоммуникация орқали жўнатилмайди.

Банкоматлар хавфсизлигини таъминлаш

Банкоматлар нақд пул олиш, ҳисоб рақамнинг ҳолати ва пул кўчириш имкониятларига эга.

Банкомат икки режимда ишлайди, off-line ва on-line.

Off-line режимда банкомат банк компьютерларидан мустақил ишлайди ва бажариладиган транзакциялар ҳақидаги ёзувларни ўз хотирасида сақлайди ҳамда принтерга узатиб, уларни чоп қилади.

On-line режимда банкомат бевосита банк компьютерлари билан телекоммуникация орқали уланган бўлади. Транзакциясини амалга ошириш мақсадида банкомат банкдаги компьютер билан қуйидаги хабарлар билан алмашади:

- банкомат сўровномаси;
- банкнинг жавоб хабари;
- банкоматнинг тўловни бажарганлиги хакидаги хабарни бериш.

Ҳозирги кунда банкоматлар тармоқларидан бир неча банкларгина фойдаланади. Бу ерда мавжуд бўлган асосий муаммо бу банкларнинг махфий ахборотларини (масалан, махфий калит) бир-биридан ҳимоялашдир.

Ушбу муаммонинг ечими сифатида PIN кодни, марказлаштирилган ҳолда, ҳар бир банк томонидан текшириш таклиф қилинади.

Бундан ташқари банкоматлар тармоғи зоналарга тақсимланади ва ҳар бир зонада **ZCMK (Zone Control Master Key)** калитлари, ўз навбатида, компьютер тармоғидаги калитларни шифрлашда қўлланилади. Маълумотларни шифрлашда эса **IWK (Issuer Working Key)** калитлар ишлатилади.

Internetда мавжуд электрон тўловлар хавфсизлигини таъминлаш

Ҳозирги кунда Internetда кўпгина ахборот марказлари мавжуд, масалан, кутубхоналар, кўп соҳали маълумотлар базалари, давлат ва тижорат ташкилотлари, биржалар, банклар ва бошқадар.

Internetда бажариладиган электрон савдо катта аҳамият касб этмокда. Буюртмалар тизимининг кўпайиши билан ушбу фаолият яна кескин ривожланади. Натижада, харидорлар бевосита уйдан ёки офисдан туриб, буюртмалар бериш имконига эга бўлишади. Шу боис хам, дастурий таъминотлар ва аппарат воситалар ишлаб чиқарувчилар, савдо ва молиявий ташкилотлар ушбу йўналишни ривожлантиришга фаол киришишган. **Электрон** савдо-глобал ахборот тармоқлари оркали махсулотларни сотиш ва пулли хизматлар кўрсатиш демакдир. **Электрон савдонинг асосий турлари қуйидагилардир:** ахборотлар сотуви; электрон дуконлар;электрон банклар.

Ахборотлар сотуви асосан маълумотлар базасидан **On-line** режимда фойдаланиш учун тақдим этилиши мумкин. Электрон дуконлар **Internetда Web-site** орқали ташкиллаштирилади. Бунда товарлар руйхати, тўлов воситалари ва бошқалар келтирилади. Харид қилинган махсулотлар оддий почта орқали жўнатилиши ёки агар улар электрон махсулот бўлса, бевосита Internetдан манзилга етказишшши мумкин.

Электрон банкларни ташкил этишдан асосий максад банкнинг доимий харажатларини камайтириш ва кенг оммани қамраб олишдир. Шу боис, электрон банклар ўз мижозларига юқори фоиз ставкаларини таклиф килишлари мумкин.

Мавзу. Компьютер тизимларининг ҳимояланганлик даражасини аниқлаш воситалари

1. SSS –System security Scanner дастури ва унинг асосий вазифалари
2. Satan ва Internet Scanner SAFE дастури ва унинг вазифалари
3. Internet Scanner SAFFEsuite дастури ҳақида

Компьютер тизимларининг ҳимояланганлик даражасини аниқлаш воситалари

Корхоналарда жорий этилаётган автоматлаштирилган ахборот тизимининг хавфсизлигини таъминлаш, биринчи навбатда, ушбу тизимни лойиҳалаш боскичида кўзда тутилган бўлиши лозим. Корхона микёсида қабул қилинган хавфсизлик сиёсатининг ахборот тизимида қандай даражада акс эттирилиши мухим масалалардан бири ҳисобланади. Лекин, ахборот-коммуникациялар технологияларининг кескин ривожланиши, ахборот оқимлари ҳажмининг ошиши **Internet** ва **Intranet** технологияларининг кенг микёсда кириб келиши бевосита автоматлаштирилган ахборот тизимларининг ахборот захираларини ҳимоялашга йўналтирилган воситаларнинг мавжудлигини таъминлаш ҳамда тизимда мавжуд бўлган ҳимоя воситаларини ривожлантиришини тақозо этади.

Автоматлаштирилган ахборот тизимларига нисбатан мавжуд бўлган хавфларни учта йўналиш бўйича ажратиш мумкин:

- амалий дастурлар;
- тармоқ хизматлари;
- операцией тизим хизматлари.

Амалий дастурларни текшириш бўйича ҳозиргача ягона восита мавжуд эмас. Тармоқ хизматлари ва операцион тизим хизматларида қўлланиладиган технологиялар умумий асосларга эга бўлганлиги учун уларни текшириш воситалари ишлаб чиқилган.

Шу боис операцион тизимни танлашда ундаги камчиликларни тахлил қилиш, ишлаб чиқарувчи фирма томонидан йўл қуйилган хатоларнинг тан олиниши ва уларни зуддик билан тузатишга киришилиши талаб этилади.

Операцион тизимнинг параметрларининг тугри ўрнатилганлигини ёки уларнинг ўзгармаганлигини текшириш учун «тизим хавфсизлигини сканерлаш» деб номланувчи 10 га яқин махсус дастурлар ишлаб чиқарилган.

Масалан, Solaris операцион тизими учун мўлжалланган ASET,Netware ва NT учун KSA, Unix учун SSS дастурлари мавжуд.

SSS(System Secyrity Scanner) дастури

Ушбу дастур **Unix** операцион тизими ўрнатилган компьютерларда хавфсизлик ҳолатини текшириш ва операцион тизимнинг ташқи ҳамда ички заиф қисмларини аниқлашга йўналтирилган. Бундан ташқари у кириш ҳуқуқларини, файлларга эгалик қилиш ҳуқуқларини, тармоқ, захираларини конфигурациялашни, аутентификациялаш дастурларини ва бошқаларни тек-шириши мумкин.

Дастурнинг қуйидаги имкониятлари мавжуд:

- конфигурациями **текшириш,** яъни рухсатсиз киришларнинг олдини олиш мақсадида конфигурацияни текшириш. Бунга қуйидагилар киради: конфигурация файллари, операцион тизим версияси, кириш ҳуқуқлари, фойдаланувчиларнинг захиралари, пароллар.

- **тизимдаги хавфли** ўзгаришларни **текшириш.** Рухсатсиз киришлар оқибатида тизимда содир бўлган ўзгаришларни қидиришда қўлланилади.

Бундай ўзгаришларга қуйидагилар киради: файллар эгаллаган хотира ҳажмининг ўзгариши, маълумотларга кириш ҳуқуқи ёки файлдаги маълумотларнинг ўзгариши, фойдаланувчиларнинг захираларга кириш параметрларининг ўзгариши, файлларни рухсатсиз бошқа бир ташки компьютерларга узатишлар;

- **фойдаланувчи интерфейсининг қулайлиги. Бу** интерфейс ёрдамида нафақат дастур билан қулай ишлаш таъминланади, балки бажарилган ишлар бўйича ҳисоботлар ҳам яратилади;
- **масофадан сканерлаш.** Тармоқдаги компъютер-ларни текшириш ва алоқа жараёнида маълумотларни шифрлаш имконияти таъминланади;
- **ҳисоботлар тузиш.** Бажарилган ишлар бўйича тўлиқ ҳисоботлар яратилади. Ушбу ҳисоботларда тизимнинг аникданган заиф бўғинларининг изоҳи келтирилади ва уларни тузатиш бўйича кўрсатмалар берилади. Хисобот HTML ёки оддий матн кўринишида бўлиши мумкин.

SATAN дастури ҳақида

Тармоқ, хизматларининг ҳимояланганлигини таҳлил қилиш бўйича биринчи бўлиб ишлаб чиқарилган дастурлардан бири бу **SATAN** дастуридир. Бу дастур 20 га якин тармоқ хизматларидаги заифликларни аниклай олади.

Internet Scanner SAFFEsuite дастури ҳақида

Агар текширувлар доимий равишда ва тўлиқ амалга оширилиши талаб қилинса, у ҳолда **Internet Scanner SAFFEsuite** дастурлар пакети таклиф қилинади. Бу дастурлар пакети ёрдамида 140 та маълум бўлган заифликлар ва тармоқ воситалари, яъни тармоқлараро экранлар, Web-серверлар, Unix, Windows 9.x, Windows NT тизимли серверлар ва ишчи станциялар, умуман TCP/IP протоколи қўлланиладиган барча воситалар тек-ширил ади.

Internet Scanner SAFFEsuite пакетининг умумий имкониятлари қуйидагилардан иборат:

1.Автоматлаштирилган ва конфигурацияланган сканерлаш:

- автоматлашган идентификациялаш ва заиф қисмлар бўйича ҳдообот тузиш;
- доимий режа бўйича сканерлаш;
- IP манзилларни сканерлаш;
- фойдаланувчи ўрнатган параметрларни сканерлаш;
- заиф бугинларни автоматик равишда тузатиш;
- ишончлилик ва такрорланувчанликни таъминлаш.

2.Хавфсизликми таъминлаш:

- тармоқ воситаларини инвентаризациялаш ва мавжуд асосий заиф бўғинларни идентификациялаш;
- асосий ҳисоботларни такослаш ва келгусида улардан фойдаланиш учун таҳлил қилиш.

3.Фойдаланишнинг оддийлиги:

- фойдаланувчининг график интерфейси;
- HTML туридаги тартибланган ҳисоботларни яратиш;

ЎЗБЕКИСТОН РЕСПУБЛИКАСИ ҚИШЛОҚ ВА СУВ ХЎЖАЛИГИ ВАЗИРЛИГИ

САМАРҚАНД ҚИШЛОҚ ХЎЖАЛИГИ ИНСТИТУТИ

ОЛИЙ МАТЕМАТИКА ВА АХБОРОТ ТЕХНОЛОГИЯЛАРИ КАФЕДРАСИ

«КОМПЬЮТЕР ТИЗИМЛАРИДА АХБОРОТЛАРНИ ҲИМОЯЛАШ»

фанидан

_____ЛАБОРАТОРИЯ ИШИ №_____

Мавзу:_____

_____

Бажарди: иқтисодиёт ва бошқарув факультети 2- боскич, 20__ гуруҳ талабаси_____

Текширди. Олий математика ва ахборот технологиялари кафедраси доценти Ҳ. Урдушев

Самарқанд 2009

ЎЗБЕКИСТОН РЕСПУБЛИКАСИ ҚИШЛОҚ ВА СУВ ХЎЖАЛИГИ ВАЗИРЛИГИ

САМАРҚАНД ҚИШЛОҚ ХЎЖАЛИГИ ИНСТИТУТИ

ОЛИЙ МАТЕМАТИКА ВА АХБОРОТ ТЕХНОЛОГИЯЛАРИ КАФЕДРАСИ

«КОМПЬЮТЕР ТИЗИМЛАРИДА АХБОРОТЛАРНИ ҲИМОЯЛАШ»

фанидан

МУСТАҚИЛ ТАЪЛИМ БЎЙИЧА РЕФЕРАТИ

МУСТАҚИЛ ТАЪЛИМ №_____

Мавзу:_____

_____

Бажарди: иқтисодиёт ва бошқарув факультети
2- босқич, 20__ гуруҳ талабаси_____

Текширди. Олий математика ва ахборот технологиялари кафедраси
доценти М. Рахимов

Самарканд 2009

Иқтисодиёт ва бошқарув факультети 2 босқич 2_____ гурух талабаси

_____ нинг

ШАХСИЙ КУТУБХОНАСИ

Ҳ.Урдушев, М.Рахимов. Компьютер тизимларида ахборотларни ҳимоялаш фанидан амалий, лаборатория иши ва мустақил таълим вазифаларини бажариш учун мажмуа. Самарқанд 2009 йил. Хажми 6,8 босма табоқ. 108 бет. Тиражи 100 нусха

«Иқтисодиёт» ва «Фермер хўжалигини бошқариш» йўналишларида таълим олаётган бакалавлар учун

Услубий мажмуа: СамҚХИ «Олий математика ва ахборот технологиялари» кафедрасида (___.___. 200__ йил, мажлис баёни № __), Иқтисодиёт ва бошқарув факультетининг Услубий (___.___. 200__ йил, мажлис баёни №__) ва Илмий кенгашида (___.___. 200__ йил, мажлис баёни №___), институт Марказий ўқув - услубий кенгашида (___.___. 200__ йил, мажлис баёни №___) муҳокама қилинган ва фан бўйича машғулотларда фойдаланишга тавсия қилинган.

Самарқанд 2009 йил. Хажми 6,8 босма табоқ. 108 бет. Мажмуа «Олий математика ва ахборот технологиялари кафедраси компьютерларида терилиб саҳифаланган ва кўпайтирилган

Ҳ.Урдушев, М.Рахимов.

Компьютер тизимларида ахборотларни ҳимоялаш фанидан амалий, лаборатория иши ва мустақил таълим вазифаларини бажариш учун мажмуа

2500 125